(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年11月1日 (01.11.2001)

PCT

(10) 国際公開番号
WO 01/82086 A1

(51) 国際特許分類[7]: G06F 12/00, 13/00, 15/00

(21) 国際出願番号: PCT/JP01/03515

(22) 国際出願日: 2001年4月24日 (24.04.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-122681 2000年4月24日 (24.04.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-0000 大阪府門真市大字門真1006番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 上田真臣 (UEDA, Masaomi) [JP/JP]; 〒336-0015 埼玉県浦和市太田窪2012-2 Saitama (JP). 石川 晃 (ISHIKAWA, Akira) [JP/JP]; 〒214-0022 神奈川県川崎市多摩区堰2-12-3 301 Kanagawa (JP). 三藤 隆 (MITOH, Takashi) [JP/JP]; 〒819-1112 福岡県前原市浦志482-1-202 Fukuoka (JP).

(74) 代理人: 二瓶正敬(NIHEI, Masayuki); 〒160-0004 東京都新宿区四谷2丁目12-5 第6冨沢ビル6階 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

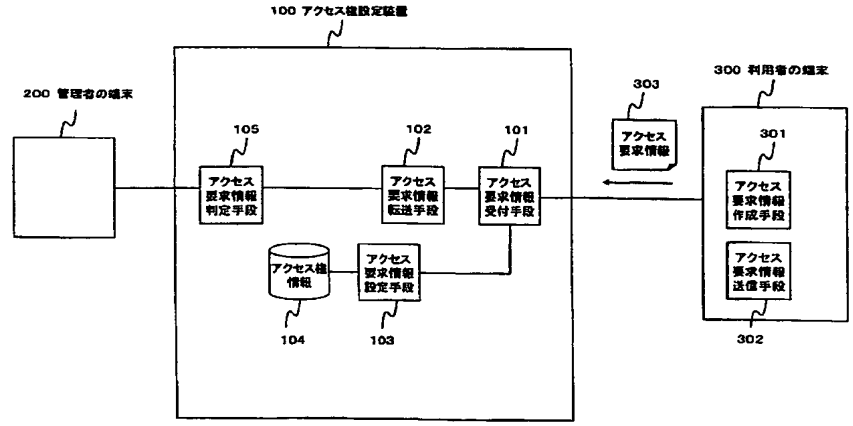
(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

[続葉有]

(54) Title: ACCESS RIGHT SETTING DEVICE AND MANAGER TERMINAL

(54) 発明の名称: アクセス権設定装置及び管理者端末



200...MANAGER TERMINAL
100...ACCESS RIGHT SETTING DEVICE
105...ACCESS REQUEST INFORMATION JUDGING MEANS
104...ACCESS RIGHT INFORMATION
103...ACCESS REQUEST INFORMATION SETTING MEANS
102...ACCESS REQUEST INFORMATION TRANSFER MEANS
101...ACCESS REQUEST INFORMATION RECEIVING MEANS
303...ACCESS REQUEST INFORMATION
300...USER TERMINAL
301...ACCESS REQUEST INFORMATION CREATING MEANS
302...ACCESS REQUEST INFORMATION TRANSMITTING MEANS

(57) Abstract: An access right setting device for readily setting an access right when a user of which the access to a resource of a network is limited makes a request and a system including a manager terminal are disclosed. In the system, a user who requests an access to a resource describes the contents of setting of an access right such as the resource, time, and access content in access request information (303) and sends it to an access right setting device (100) managing an access right, the received access request information (303) is transferred to the manager of the resource by an access request information transfer means (102), the manager confirms the content of the request and makes a judgement of approval, and thus the access right setting device (100) automatically sets an access right.

[続葉有]

WO 01/82086 A1

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

ネットワークの資源へのアクセスを制限された利用者が要求を出すことで、簡単にアクセス権の設定が行えるアクセス権設定装置及び管理者端末を含むシステムが開示され、同システムでは、資源へのアクセスしたい利用者が、資源、時間、アクセス内容などのアクセス権の設定内容をアクセス要求情報３０３に記述し、アクセス権を管理するアクセス権設定装置１００へ向けて送信する。受け取ったアクセス要求情報３０３は、アクセス要求情報転送手段１０２により、資源の管理者へ転送され、管理者が要求内容を確認し承認の判断を下すだけで、アクセス権設定装置１００により自動でアクセス権の設定が行われる。

明　細　書

アクセス権設定装置及び管理者端末

技術分野

本発明は、ネットワーク上に存在する制限的に利用可能な資源を利用する利用者からの要求によるアクセス権の設定が可能なアクセス権設定装置及びそのシステムに関する。

背景技術

従来、ネットワーク上の資源を複数の利用者がアクセスする場合、その資源を管理しているコンピュータに、利用者のアクセス権の情報が保持されており、この情報を基にアクセス制御を行うことになる。ここで、利用者とは、人間、プログラム、プロセス（実際は、人間がプログラムやプロセスを作成し実行することになる）などを表し、資源とは、ファイル、メモリ、プログラム、プロセス、機器などを表す。

アクセス権情報は一般的に、各利用者単位、又は、利用者が属するグループ単位で、参照（資源の存在の確認）、読み出し（資源の内容を見る）、書き込み（資源の内容を書き変える）、消去（資源を記録媒体から消去する）、実行（プログラムを実行する）などのアクセス形態に関し、アクセスを許可するか否かの記述をする。

一般的なネットワークＯＳ（オペレーティング・システム）でのアクセス権の設定方法を説明する。ネットワークの管理者により、ユーザ（利用者）に対し、ネットワークへアクセスするのに必要なユーザＩＤ（利用者識別子）の登録が行われ、リモート・アクセスの許可設定を行うことで、アクセスが可能となる。その他、ネットワークの管理者は、アク

セス期間や、ユーザのグループ化なども設定できる。ユーザがアクセス可能な資源は、主に自らが管理しているマシン内の資源や、それぞれのマシンの管理者が外部ユーザからのアクセスを許可した資源などである。

このようなアクセス権の設定内容は、通常資源の管理者が設定を行うものので、資源の利用者は設定できない。もし資源の利用者がアクセス権のない資源へアクセスする場合は、何らかの手段でアクセス権変更の要求を管理者に伝えることになる。

又、ネットワークのユーザＩＤを持っていないユーザがアクセスする手段として、ゲストＩＤという概念がある。一般的に、ゲストＩＤでネットワークへログインするために必要なパスワードは公知であり、だれでもネットワークへアクセスできるのだが、セキュリティ上、ネットワークに障害が起きないように、アクセス可能な資源が極めて限定されている。いずれにしても、利用者がアクセス権の設定をすることはできない。

利用者が管理者へネットワーク経由でアクセス要求を伝え、アクセス権の設定を行う方式として、特開平５－００６３２２号公報がある。利用者がアクセス権を有しない資源へのアクセスを行った場合、アクセス権の変更依頼が管理者へ通知され、管理者がアクセスを許可するようなアクセス権の変更を行う、といったアクセス権の設定方式である。

本発明では、特に一般の家庭で構築される、ネットワーク家電機器を繋いだホームネットワークでの実現を考える。通常ホームネットワークで資源（ネットワーク家電機器）を管理する管理者（家庭の人）は、ネットワークの知識がない人が多く、複雑な条件のアクセス権の設定の処理が困難であると言える。又、資源の利用者としては、家庭内の人はもちろんだが、外部の事業者がサービスを提供するために資源を利用する場合が考えられる。サービス例としては、遠隔医療、遠隔監視、遠隔保

守などが挙げられる。上述の通り、管理者である家庭の人はアクセス権の設定が困難なため、利用者である外部の事業者がアクセス権の設定内容を提示し、家庭の人はアクセス権情報として登録するかの判断、又は簡単な作業を行うのみ、という簡易な設定方式を考える。

以上のようなホームネットワークを利用した上で、従来の技術における課題を挙げる。

第１の課題として、アクセス権の設定内容（アクセス権を適用する期間、アクセス内容、その他アクセスできる条件など）の指定を、管理者ではなく利用者の方で行うことができない。

第２の課題として、アクセス権設定の要求は、利用者主導でアクセス権を管理している装置へ送信しなければならない。

第３の課題として、アクセス権の管理をするのは人間でなければならず、その場にいない場合はアクセス権の設定処理が滞り、又、頻繁にアクセス権設定の要求が投げられる場合は面倒である。

第４の課題として、利用したい資源（以下、アクセス対象資源という）を保持するネットワークに対して、資源へアクセスするための通信ができない（以下、ログインできないという）利用者は、アクセス権設定の要求を出すことができない。又、管理者は、ログインするためのユーザＩＤの設定という特殊な知識が必要になる。

第５の課題として、利用者が、利用したい資源を一意に特定する識別子を知らない場合、アクセス要求情報に、アクセスを許可して欲しいアクセス対象資源を指定することができない。

第６の課題として、第３の課題を解決した場合、指定されたアクセス対象資源を、利用者側で選択することができない。

第７の課題として、第１の課題を解決した場合、利用者によるアクセス権の設定内容の指定はできるが、更に、管理者により詳細な指定を行

いたい場合もでてくる。

第８の課題として、利用者が、ネットワークにどういう資源が存在するか知りたい場合がある。

第９の課題として、第１の課題を解決した場合、利用者がアクセス要求情報を不正に作成することで、管理者（人間）へ表示した内容とは別の設定が行われる可能性がある。

第１０の課題として、第１の課題を解決した場合、利用者が指定したアクセス権の設定内容が信頼できるものか、客観的な判断が難しい。

第１１の課題として、管理者の端末が携帯端末である場合でも、第１又は、第２の課題を解決したい。

第１２の課題として、管理者の端末が携帯端末である場合でも、第６の課題を解決したい。

第１３の課題として、管理者の端末が携帯端末である場合でも、第７の課題を解決したい。

発明の開示

本発明は、以上の課題を解決するために、ネットワークのユーザＩＤを持たない利用者により、存在や識別子を知らないネットワークの資源に対して、アクセス権の設定内容（以下、利用者がアクセス権の設定要求のために指定するアクセス権の設定内容を「アクセス要求情報」と言う）を指定を行うものである。これにより、管理者に負担をかけずにアクセス権の設定が可能になり、又、利用者、並びにアクセス要求情報が信頼でき、管理者に知られずに不正にアクセス権の変更が行われないしくみも実現する。さらに、管理者により、利用者が指定したアクセス要求情報の変更が行えるしくみも実現する。

なお、特開平５－００６３２２号公報記載のアクセス権の設定方式で

は、利用者が利用したい資源の識別子を知らない場合や、利用者がネットワークのユーザＩＤを持たない場合の解決手段について言及していない。又、管理者により詳細なアクセス権の設定が行われるが、利用者にはそのアクセス権の指定内容が制限されている。

この課題を解決するために本発明は、第１に利用者が指定したいアクセス要求情報を作成する手段と、利用者が指定したアクセス要求情報を受け取る手段と、アクセス要求情報を管理者へ転送する手段と、アクセス要求情報を基に管理者が設定の可否判定を行う手段と、管理者の許可判断により、利用者が指定したアクセス要求情報をアクセス権情報として設定する手段とを備えたことより、管理者によるアクセス権の複雑な設定が必要なくなると共に、利用者によるアクセス権の設定内容の指定が可能となる。

第２に、利用者が、作成したアクセス要求情報を管理者側から見える場所に一旦保存する手段と、管理者側からこのアクセス要求情報を取得する手段を備えたことにより、管理者主導でアクセス権の設定が容易にできる。

第３に、アクセス要求情報をアクセス権情報として設定するかの可否判定を機械により自動で行う手段を、管理者の端末に備えたことにより、人間が、利用者の端末にいない場合でも、機械が自動で判定を行い、又、アクセス要求情報が頻繁に投げられる場合のような煩わしい作業も、機械での自動化で解消できる。

第４に、ネットワークへログインする際のユーザ認証で必要な利用者のユーザＩＤを作成し、アクセス権情報の一部として登録する手段を備えたことにより、ネットワークへログインできず、ユーザＩＤを持たない利用者からでも、管理者へアクセス権設定の要求が可能となる。

第５に、利用者、管理者双方で既知である、資源を抽象化した種別情

報でのアクセス対象資源の記述が行えることにより、ネットワークへログインできない利用者などが具体的な資源の識別子を知らない場合でも、アクセス権設定の要求が可能になる。

第６に、第３の解決手段で記載した、利用者が利用したいアクセス対象資源を種別の情報で指定した場合に、管理者により利用を許可する資源を選択する手段を備えたことにより、アクセス対象資源を一意に決定できるのと共に、管理者の意志が尊重されたアクセス権の設定が可能となる。

第７に、アクセス要求情報を転送する手段で管理者に提示されたアクセス要求情報に記述された内容を、管理者からも変更ができる手段を備えたことにより、利用者だけに一方的にアクセス権の設定内容が指定されることなく、管理者の意志が尊重された、より柔軟なアクセス情報の設定が可能になる。

第８に、ネットワークが備えたアクセス可能な資源の情報を、利用者が取得できる手段を備えたことにより、資源の識別子を知らない利用者でも、資源の存在や、その情報を取得することができ、アクセス要求情報へ盛り込むことが可能となる。

第９に、利用者が作成したアクセス要求情報を基に、人間である管理者に提示する自然言語による表示情報を作成する手段を備えたことにより、悪意のある利用者が不正に作成したアクセス要求情報にて、不正にアクセス権を設定されることなく、正確にアクセス要求情報の内容を管理者へ伝えることが可能となる。

以下、機械が理解できるように人間によって作られたプログラムやコードなどの表現を人工言語、人間が理解できる、音声、画像、文字などのＵＩ（ユーザ・インターフェース）情報の元となる表現を自然言語と呼ぶ。

第１０に、受け取った、信頼のおけるＣＡ（認証局）によるデジタル署名が施されてるアクセス要求情報の認証を行う手段を備えたことにより、利用者、又はアクセス要求情報が信頼のおけるもので、且つ改ざんや、なりすましの恐れがないかの判断が可能となる。

第１１に、携帯端末へ受け取ったアクセス要求情報を転送する手段と、アクセス要求情報をアクセス権情報として設定してもよいかの可否判定を、携帯端末にて行うことができる手段をアクセス権設定装置に備えたことにより、管理者が管理者の端末にいなく、外出をしているような場合でも、容易にアクセス権の設定を行うことが可能となる。

第１２に、利用者が、利用したいアクセス対象資源を種別の情報で指定した場合、携帯端末にて利用を許可する資源を選択する手段をアクセス権設定装置に備えたことにより、管理者が管理者の端末にいなく、外出をしているような場合でも、容易に対象資源の選択を行うことが可能となる。

第１３に、携帯端末用のアクセス要求情報を転送する手段で管理者に提示されたアクセス要求情報の内容を、携帯端末にて変更ができる手段を備えたことにより、管理者が管理者の端末にいなく、外出をしているような場合でも、容易にアクセス要求情報に記述されている内容の変更を行うことが可能となる。

図面の簡単な説明

図１は、本発明の第１の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図２は、図１のアクセス要求情報の一例を表す図、

図３は、本発明の第１の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

図４は、本発明の第１の実施の形態における判定画面の一例を表す図、

図５は、本発明の第１の実施の形態における判定結果の通知画面の一例を表す図、

図６は、本発明の第１の実施の形態におけるアクセス権設定の一連の動作例を表すフローチャート図、

図７は、本発明の第２の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図８は、図７のアクセス要求情報の一例を表す図、

図９は、本発明の第２の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

図１０は、本発明の第２の実施の形態におけるサービス一覧画面の一例を表す図、

図１１は、本発明の第３の実施の形態におけるアクセス権設定システムの内、管理者の端末の構成を示す図、

図１２は、本発明の第３の実施の形態におけるアクセス権設定の一連の動作例を表すフローチャート図、

図１３は、本発明の第４の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図１４は、図１３のアクセス要求情報に記述するアクセス対象資源の種別情報の一例を表す図、

図１５は、本発明の第４の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

図１６は、本発明の第５の実施の形態におけるアクセス権設定システムの内、管理者の端末の構成を示す図、

図１７は、本発明の第５の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

図１８は、本発明の第５の実施の形態におけるアクセス要求情報の内容表示画面の一例を表す図、

図１９は、本発明の第５の実施の形態における選択画面の一例を表す図、

図２０は、本発明の第６の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図２１は、図２０の公開資源情報の一例を表す図、

図２２は、図２０の公開資源の種別情報の一例を表す図、

図２３は、本発明の第６の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

図２４は、本発明の第７の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図２５は、本発明の第７の実施の形態における不正に作成されたアクセス要求情報の一例を表す図、

図２６は、本発明の第７の実施の形態における変換テーブルの一例を表す図、

図２７は、本発明の第７の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

図２８は、本発明の第７の実施の形態におけるアクセス権設定の一連の動作例を表すフローチャート図、

図２９は、本発明の第８の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図３０は、本発明の第８の実施の形態におけるアクセス権設定装置と携帯端末間の一連の動作例を表すシーケンス図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について、図１から図３０を用いて説明する。なお、本発明はこれら実施の形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施し得る。

（実施の形態１）

図１は、本発明のアクセス権設定装置及び管理者端末を含むネットワークシステム全体の第１の実施の形態の構成を表すものである。第１の実施の形態では、アクセス権の設定内容を利用者が指定できると共に、管理者はその指定内容で適切なものか判別するだけで、簡易にアクセス権の設定を行えるようにするのが目的である。

本発明のネットワークシステムは大きく、アクセス権設定装置１００、管理者の端末２００、利用者の端末３００、といった装置群から構成される。アクセス権設定装置１００は、管理している資源へのアクセスを制限するためのアクセス権の設定及び管理を行う装置である。管理者の端末２００は、利用者から要求されるアクセス権の設定内容の確認及びアクセス権の設定を行うための管理者用の端末である。なお、管理者の端末２００はリモートの端末と限定せず、アクセス権設定装置１００そのものと考えてもよいものとする。利用者の端末３００は、利用者がアクセス権設定の要求を出したり、実際にアクセスする際に用いる端末である。利用者の端末３００を用いてアクセスする利用者からは、アクセス権設定装置で管理されているネットワーク資源へ自由にアクセスできるわけではなく、アクセス権情報１０４に基づいたアクセス制御により、利用者からのアクセスが制限されることになる。なお、これらの端末群及び装置は同一機器としてもよく、その形態は特に限定しない。また、アクセス権設定装置１００にて管理されるアクセス権を用いてのアクセス制御が行われる場所も、アクセス設定装置１００のみならず、特に限定しない。なお、本発明で用いる利用者とは、人間とは限らず、機械が

自動で動く場合でもよいものとする。

まず、利用者の端末３００内の構成要素について説明する。アクセス要求情報作成手段３０１は、利用者が利用したい資源へのアクセスを許可してもらうための要求情報であるアクセス要求情報３０３を作成する手段である。このアクセス要求情報３０３は、アクセス要求情報送信手段３０２にて、アクセス権設定装置１００へ送信されることになる。

次に、アクセス権設定装置１００内の各構成要素について説明する。アクセス要求情報受付手段１０１は、利用者が作成したアクセス要求情報３０３を受け付けるための手段である。アクセス要求情報転送手段１０２は、アクセス要求情報受付手段１０１で受け付けたアクセス要求情報３０３の内容を管理者の端末へ転送する手段である。なお、内容の転送は図１のようにリモートの端末だけではなく、アクセス権設定装置１００内のローカルでの転送でもよく、以後ローカル転送の例を説明する。アクセス要求情報設定手段１０３は、管理者がアクセス要求情報の内容を許可した場合に、アクセス権情報１０４として設定を行うための手段である。

アクセス要求情報判定手段１０５は、アクセス権設定装置１００のアクセス要求情報転送手段１０２により転送されたアクセス要求情報３０３の内容を、アクセス権情報１０４として設定するかどうかの判定を行うための手段である。この手段で設定が許可されれば、アクセス要求情報設定手段１０３により、アクセス権情報１０４として設定されることになる。なお、アクセス要求情報判定手段１０５は、アクセス権設定装置１００ではなく、リモートの端末にあってもよいものとする。

利用者により作成されるアクセス要求情報３０３の一例を図２に示す。アクセス要求情報３０３は、利用者とアクセス権設定装置１００同士で通信を可能にするため、双方で理解し得る共通の通信規約（プロトコル）

に則って作成されるものであり、コンピュータが理解できる人為的に作られた例えばＸＭＬ（Extensible Markup Language）のような人工言語として記述される。

図２に示される各項目の説明を行う。「利用者」はネットワークを利用する利用者を一意に識別する識別子（ネットワークのユーザＩＤのことを言う）を表し、利用者がネットワークへのアクセスを許可されているかどうかの判断（ユーザ認証）を行う場合、又は管理者へどの利用者からの要求かを通知したい場合などに用いられる。「利用端末」は、利用者が資源へアクセスする際に使用する端末の場所(ネットワークアドレス)を表しており、該当する端末からのみアクセス可能と、制限を加える場合に用いる。「期間」は、アクセスが可能となる期間を表し、期間の制限を加えたい場合に用いる。「アクセス対象資源」は、利用者がアクセスを許可して欲しい資源を表す。「アクセス内容」は、利用者がアクセスを許可して欲しい内容を表す。以上の項目から、利用者によるアクセス権の設定内容の指定が可能となる。図２で挙げた項目は一例であり、この他に必要な項目があれば、アクセス要求情報の一部として追加しても構わないものとする。又、図２記載の項目は任意であり、すべてが必要という訳ではない。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図３に、アクセス権設定装置１００、管理者の端末２００、利用者の端末３００間での動作例を示す。利用者が、アクセス要求情報作成手段３０１により、前記通信規約に則って、アクセス要求情報３０３が作成される（1００１）。利用者によって作成されたアクセス要求情報３０３は、アクセス要求情報送信手段３０２により、アクセス権設定装置１００へ向けて送信される。ここで、アクセス権設定装置１００へ送信する

際に必要なアドレスなどの情報は、利用者側であらかじめ既知であるものとする。送信されたアクセス要求情報３０３は、アクセス権設定装置１００のアクセス要求情報受付手段１０１により受け付けられる。アクセス要求情報３０３を単独で送信してもよいし、アクセス権設定装置１００内で動作させるためのアプリケーション・プログラムなどと一緒に送信してもよいものとする。なお、アクセス要求情報受付手段１０１は、アクセス要求情報３０３に記載された通信規約を知っており、理解することができるものとする。ただし、アクセス要求情報３０３は、不正にアクセス権情報１０４として設定されないように、信頼のおける情報とする（１００２）。

受け取ったアクセス要求情報３０３は、アクセス要求情報受付手段１０１からアクセス要求情報転送手段１０２に渡され、アクセス要求情報判定手段１０５へその内容が転送される。アクセス要求情報転送手段１０２は、あらかじめ転送先を知っているものとし、ネットワークで繋がっていて転送可能であれば、コンピュータ、ネットワーク家電など、種類、及び数量は特に限定しない。なお、特にあらかじめ転送先を知らなくても、利用者がアクセス要求情報３０３に転送先（管理者の指定、又は転送端末の指定）を記述することで、転送先の指定も可能とする（１００３）。

転送されたアクセス要求情報３０３の内容は、アクセス権設定装置１００のアクセス要求情報判定手段１０５により、アクセス権情報１０４として設定するかどうかの判定が行われる。判定は管理者である人間により行われるもので、例えば、管理者の端末２００上に、アクセス要求情報３０３の内容が表示され、その表示内容を参照し判定を行うことになる。なお、表示形式としては、利用者がアクセス要求情報に盛り込んだ、文字、音声、画像などの、人が理解し易い自然言語の表示形式、又

は、機械向けの人工言語の内容をそのまま表示することになる。

図４に、管理者の端末２００に表示される判定画面の例を示す。図４は、図２に示すアクセス要求情報３０３の内容を表示したもので、文字及びボタンなどのＵＩ（ユーザー・インターフェース）情報を用いた自然言語による表現となる。

この自然言語は、利用者によりアクセス要求情報の一部として記述されるか、又は別に画面表示用のプログラムを用意するなどして表示される。管理者としては、表示された内容に対して許可判定を行う（図４の例では、許可、不許可のどちらかのボタンを押す作業）だけなので、アクセス権の細かな指定をする必要がなくなり、簡易に設定を行うことができる。ただし、利用者の身元及びアクセス権の指定内容は、あまり知識のない管理者では判定が難しいかもしれないので、この場合は、熟練した専門家に判定を依頼するような、判定代行のモデルも考えられる（１００４）。アクセス要求情報３０３が許可された場合、その情報がアクセス権設定装置１００のアクセス要求情報受付手段１０１まで返る（１００５）。判定結果を受けたアクセス要求情報受付手段１０１はアクセス要求情報設定手段１０３へアクセス権情報１０４への設定を依頼することで、結果としてアクセス要求情報３０３が、アクセス権情報１０４として設定される（１００６）。無事に設定された旨を、設定内容と共に、利用者の端末へ通知する。

図５に、利用者への通知画面の例を示す。なお、図５のようにアクセス権の設定内容の詳細まで通知しなくてもよく、設定可否の旨だけを通知してもよい（１００７）。

以下に説明する構成要素は図１に示していないが、設定されたアクセス権情報１０４を基に、どのようにアクセス制御が行われるかの説明を行う。なお、例としてアクセス制御はアクセス権設定装置１００内で行

われているとするが、特にアクセス制御が行われる場所は問わない。まず、利用者の端末から対象資源へのアクセスが起こる。なお、１００２のアクセス要求の動作で説明した通り、アクセス要求情報３０３は、アクセス権設定装置１００内で動作するアプリケーション・プログラムなどと送信してもよく、この場合は、アクセス制御による資源の利用制限を受ける利用者をアプリケーション・プログラムに置き換えることができる（１００８）。アクセス権情報１０４として設定されているユーザＩＤ情報を基に、利用者がネットワークへのアクセスを許可されているかどうかの判断であるユーザ認証を行う。認証の手段としては、パスワードを利用した手段などが考えられる（１００９）。アクセス権情報１０４として設定された、「利用端末」、「期間」、「アクセス対象資源」、「アクセス内容」などを基に、アクセス権設定装置１００により、アクセス対象資源へのアクセス可否の判定をするアクセス権のチェックが行われる（１０１０）。この結果、アクセスが許可された場合には、対象資源へのアクセスが可能となる（１０１１）。

図６に、アクセス権の設定が行われるまでのフローチャートを示す。利用者が作成したアクセス要求情報３０３を受け付ける（１１０１）。アクセス要求情報３０３を理解し、管理者の端末２００へ転送する（１１０２）。管理者がアクセス要求情報３０３の許可判定を行う（１１０３）。許可された場合は、アクセス要求情報３０３を設定し（１１０４）、その結果が利用者へ通知される（１１０５）。許可されない場合は、アクセス要求情報３０３は設定されず（１１０６）、不許可の結果が利用者へ通知される。図６に利用者への通知の例を示す（１１０７）。

上述のように構成された本発明の第１の実施の形態によれば、従来は管理者によって決められていたアクセス権が、利用者によって指定できるようになり、逆に、管理者は煩わしいアクセス権の設定がなくなって、

管理者の負担が軽減される。特に、ネットワーク対応の家電・ＡＶ機器を繋いで構成されるホームネットワークについて考えると、管理者である家庭の人はネットワークの知識があまりないことから、アクセス権の設定が簡易に可能になる本発明は有効な方式であると言える。又、ホームネットワークと外部のインターネット網とを接続することで、不特定多数の利用者から、頻繁に複雑な設定が必要とされる点が考えられ、有効なシステムであるといえる。

（実施の形態２）

図７は、本発明第２の実施の形態におけるネットワークシステム全体の構成を表すものである。第２の実施の形態では、利用者の端末からアクセス要求情報を送信しなくても、アクセス権設定装置側からアクセス要求情報を取得することを目的とする。

図１に示す第１の実施の形態では、利用者の端末３００からアクセス要求情報３０３を送信し、アクセス権設定装置１００へ伝えていたが、本実施の形態では管理者の依頼により、アクセス権設定装置１００が、ある場所に保存されているアクセス要求情報３０３を取得しにいく手段を備えた点が異なる。

本実施の形態の構成を図７を用いて説明する。ただし、実施の形態に記載のネットワークシステムと同様に、アクセス権設定装置１００、管理者の端末２００、利用者の端末３００にて構成されており、一部の機能は同じものであるので、異なる点についてのみ説明する。なお、以下管理者の端末２００はリモートの端末と限定せず、アクセス権設定装置１００そのものと考えてもよいものとする。

利用者の端末３００には、アクセス要求情報作成手段３０１により作成したアクセス要求情報３０３を保存するために用いるアクセス要求情報保存手段３０４を備える。保存先として、利用者の端末から通信可能

なネットワーク上にアクセス要求情報蓄積装置４００が存在する。アクセス権設定装置１００には、アクセス要求情報蓄積装置４００に蓄積されているアクセス要求情報３０３を取得し、受け付けるために用いるアクセス要求情報受付手段１０１を備える。又、アクセス権設定装置１００には、アクセス要求情報３０３の取得処理をアクセス要求情報判定手段１０５へ依頼するアクセス要求情報取得依頼手段１１４を備える。なお、アクセス要求情報取得依頼手段１１４は、アクセス権設定装置１００ではなく、リモートの端末にあってもよいものとする。

ホームネットワークには、ネットワークに対応した家電・ＡＶ機器が接続されており、この機器を外部から制限的に利用可能な資源と仮定する。利用者を警備会社とし、ホームネットワークに接続されているビデオカメラへアクセスすることで、留守宅の映像を取得する遠隔監視サービスの例を考える。この例は言い換えれば、ホームネットワークへサービスを提供していると言うことができる。一般的に、ホームネットワークの管理者（家庭の人を意味する）は、コンピュータ及びネットワークの知識を有していないと考えられ、複雑なアクセス権の設定は困難である。又、提供されるサービスも多種多様であり、ホームネットワークの家庭の人とは異なる部外者（コンピュータネットワークで言うところのゲスト）が資源の利用者となり、より一時的なアクセスが要求される。

以上の点からも、ホームネットワークへサービスを提供する利用者（事業者）へのアクセス権の付与を考えた場合、通常のコンピュータネットワークのアクセス権の設定よりも多種多様な用途が考えられ、更に複雑な設定が必要となる。従って、第１の実施の形態に記載の、「管理者に複雑な設定を行わせず」に、「利用者によるアクセス権の設定内容の指定が可能」な、アクセス権の設定のしくみの必要性が高まると言える。

ホームネットワークへ提供されるサービスの一例として、上述した警

備会社による遠隔監視サービスを用いて以下説明する。

遠隔監視サービスの場合のアクセス要求情報３０３の例を図８に示す。「利用者」は、利用者を特定するための識別子であるユーザＩＤを示しており、ネットワークへログインする際の認証時に利用者を識別するために用いられるものである。警備会社Ａが複数のサービスを提供する場合も考えらるので、利用者を識別するユーザＩＤを、利用者毎というよりは、サービス毎に作成した方が望ましい。「属性」は、利用者、又はサービスが属するグループを示しており、グループ単位でのアクセス制御を行う場合に必要となる。「利用端末」、「期間」、「アクセス内容」は、第１の実施の形態での説明と同じであるため、ここでは省略する。「アクセス対象資源」は、利用者が利用したい資源を表しており、ここで「ビデオカメラＢ」は、ホームネットワークに接続されている機器を一意に特定できる識別子（ネットワークアドレス、具体的な資源名など）を指定して表している。最後に「条件」は、その他の時間的に変化の伴う要因に依存したアクセス権情報１０４で、例えば「警報センサ反応時」の場合は、侵入物によるセンサ反応時のみ監視を行わせるためにアクセスを許可し、それ以外の正常時にはアクセスを許可しないといった、詳細で柔軟な設定も可能になる。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図９に、アクセス権設定装置１００、管理者の端末２００、利用者の端末３００、アクセス要求情報蓄積装置４００間での動作例を示す。この例では、アクセス要求情報判定手段１０５、及びアクセス要求情報取得依頼手段１１４が管理者の端末２００にある場合として説明する。図９は、図１に示す第１の実施の形態における動作例に新たな動作１２０２～１２０５を加えたものであり、残りの１２０１は、１００１に、１

２０６～１２１３は１００４～１０１１にそれぞれ対応しているため、ここでは説明を省略する。

利用者がアクセス要求情報作成手段３０１にて作成したアクセス要求情報３０３を、アクセス要求情報保存手段３０４を用いてアクセス要求情報蓄積装置４００へ保存する（１２０２）。

なお、アクセス要求情報蓄積装置４００は、利用者の端末３００及びアクセス権設定装置１００から通信可能であればよく、特に設置されている場所は限定しない。管理者は、管理者の端末２００からアクセス権設定装置１００のアクセス要求情報取得依頼手段１１４へアクセスし、アクセス権設定装置１００のアクセス要求情報取得手段へ向けて、アクセス要求情報蓄積装置４００に蓄積してあるアクセス要求情報３０３の取得の依頼を行う。なお、管理者は、アクセス要求情報蓄積装置４００に存在するアクセス要求情報３０３の一覧を見るなどして、あらかじめ取得したいアクセス要求情報３０３を知っているものとする。

図１０にホームネットワークに導入するサービス一覧画面の例を示す。各サービスに対応するアクセス要求情報３０３が、アクセス要求情報蓄積装置に存在することを意味する。図１０の例で、もし管理者である家庭内の人が、サービス一覧から遠隔監視サービスを選択した場合、遠隔監視サービスのアクセス要求情報３０３を取得するための依頼コマンドが、アクセス権設定装置１００のアクセス要求情報取得手段まで投げられることになる（１２０３）。管理者から依頼されたアクセス要求情報受付手段１０１は、該当するアクセス要求情報３０３をアクセス要求情報蓄積装置４００から取得する。この際、アクセス要求情報３０３を単独で取得してもよいし、アクセス権設定装置１００内で動作させるためのアプリケーション・プログラムなどと一緒に取得してもよいものとする。

アプリケーション・プログラムと一緒に取得した場合、アクセス要求

情報３０３に記述されたアクセス権設定の内容は、利用者及びアプリケーション・プログラムに対する利用したい資源へのアクセス権の内容となる（１２０４）。アクセス要求情報受付手段１０１は、取得したアクセス要求情報３０３をアクセス要求情報転送手段１０２へ渡され、管理者の端末２００へその内容が転送される（１２０５）。

上述のように構成された本発明の第２の実施の形態によれば、利用者がアクセス権設定の要求を投げることなく、管理者側からアクセス要求情報を取得できることで、上述のホームネットワークのサービスを導入する例のように、管理者が希望するときに、簡易にアクセス権の設定を行うことが可能になる。又、利用者から一方的に送信されることなく、管理者の意思に従ってアクセス要求情報を取得しにいくので、不正アクセスを招く可能性が低くなるという効果もある。

（実施の形態３）

図１１は、本発明第３の実施の形態におけるネットワークシステム全体の構成のうち、新たに手段を追加した管理者の端末の構成を表すものである。第３の実施の形態では、管理者が人間ではなく、機械により自動で、アクセス要求情報をアクセス権情報１０４として設定するかの可否判定を行うことを目的とする。

図１に示す第１の実施の形態におけるアクセス権設定装置１００の構成と異なり、図１１では、機械によりアクセス要求情報をアクセス権情報１０４として設定する可否判定を行うアクセス要求情報自動判定手段２０３を管理者の端末２００に備えている。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図１２に、アクセス権の設定が行われるまでのフローチャートを示す。アクセス要求情報３０３を受け付ける及び取得する動作は、第１及び第

２の実施の形態にて説明した通りであるので、ここでは説明を省略する。

アクセス要求情報３０３を管理者の端末へ転送する（１３０１）。転送する際、判定モードの確認を行う（１３０２）。この判定モードは、人間による判定と機械による判定のどちらで行うかを示しているもので、管理者によりあらかじめ設定されているものとする。なお、設定がされていない場合でも、デフォルト値があらかじめ設定されているものとする。もし判定モードが自動であれば、アクセス要求情報自動判定手段２０３にてアクセス要求情報３０３の可否判定が行われる。機械による判定の場合は、判定基準となるアルゴリズムが、あらかじめアクセス要求情報自動判定手段２０３に登録されていることになり、このアルゴリズムにより、転送されてきたアクセス要求情報３０３に記述されている内容を把握し、自動でアクセス権情報１０４として設定するかの可否判定が行えるものとする（１３０３）。なお、この判定基準となるアルゴリズムについては特に限定しないので、ここでは触れない。もし判定モードが自動でない場合は、アクセス要求情報判定手段２０１にてアクセス要求情報３０３の可否判定が行われる（１３０４）。仮に、管理者が端末にログインしていない場合、又は端末が起動していなかった場合などのように、管理者が判定をできる状態ではないとアクセス権設定装置１００が判断できれば、判定の処理をアクセス要求情報自動判定手段２０３に切り替える処置を取ってもいいものとする。アクセス要求情報判定手段２０１による可否判定処理は第１の実施の形態で説明しているので、ここでは省略する。又、アクセス要求情報自動判定手段２０３及びアクセス要求情報判定手段２０１の双方で判定した結果の処理１３０５～１３０８は、第１の実施の形態の図６のフローチャートの１１０４～１１０７にて説明しているので、ここでは省略する。

上述のように構成された本発明の第３の実施の形態によれば、アクセ

ス要求情報に記述された内容をアクセス権情報として設定するかの可否判定を、機械により自動で行うことにより、管理者が端末にいない場合でも自動でアクセス権の設定が行える。又、複雑なアクセス権の内容のアクセス要求情報を頻繁に判定しなければならない場合には、判定を自動モードに切り替えることにより、管理者に手間がかからずにアクセス権の設定を行うことも可能になる。

（実施の形態４）

図１３は、本発明第４の実施の形態におけるネットワークシステム全体の構成を表すものである。第４の実施の形態では、ネットワークへログインすることのできない利用者からでも、アクセス権設定の要求を受け付け、ログインするために必要な利用者を一意に確定する識別子（以下、ユーザＩＤと言う）を発行することを目的とする。

図１に示す第１の実施の形態の構成図と異なり、図１３に示すネットワークシステムでは、ローカルネットワーク５００にログインするために必要なユーザＩＤを持たない利用者（の端末）からのアクセス要求を考え、アクセス権設定装置１００内に、利用者の識別子（ユーザＩＤ）を発行し、アクセス権情報１０４の一部として登録する利用者識別子登録手段１０６を備えている。なお、管理者の端末２００及び利用者の端末３００の構成は変わっていない。

以下、分かり易く説明するために、ローカルネットワーク５００の例として、第３の実施の形態でも触れたホームネットワークの遠隔監視サービスの例を用いて説明をする。

外部のネットワークと接続されているホームネットワークは、外部からの不正アクセスを防ぐためにアクセス権の設定によるアクセス制御、又は、アクセスの拒否などの制限が必要である。以下、図１３に示すローカルネットワーク５００をホームネットワークと置き換え、外部のネ

ットワークの利用者が利用者の端末３００を用いてホームネットワークの資源を利用すると考える。つまり、外部の利用者が、遠隔監視サービスを提供する警備会社とする。サービスを導入する前の警備会社は部外者であり、通常ホームネットワークへのログイン及び資源へのアクセスが許可されておらず、ホームネットワークへログインするためのユーザＩＤを持っていない状態であるといえる。利用者からの要求によるアクセス権の設定を実現するためには、このようなユーザＩＤをあらかじめ持っていない利用者からでも、アクセス要求情報３０３によるアクセス権の設定要求が行える枠組みをつくる必要がある。

利用者がネットワークのユーザＩＤを持っていない部外者である場合、ネットワークにログインできずに、ネットワークがどういう資源を保持しているのか分からないケースが多いといえる。つまり、ネットワークを一意に特定する識別子が分からないことになるので、図８に示すように、アクセス要求情報３０３に記述するアクセス対象資源を指定することができない。この問題を解決するために、アクセス対象資源の識別子を抽象化した種別の情報で指定可能とする。分かり易い例として、ホームネットワークに対応したビデオカメラの指定の仕方を図１４に示す。「アクセス対象資源」を「ビデオカメラ全部」、「ビデオカメラ１台」、「Panasonic 製のビデオカメラ」のように抽象化して種別（以下、種別情報という）での指定を行うものとする。ただし、利用者側で指定された資源が、管理者（アクセス権設定装置）側で理解されなければいけないため、種別情報による指定は、その資源の表記が規格化され一般的に（又は、利用者と管理者の間で）認知されている場合に用いることができる。例えば、あるホームネットワークの規格では、ビデオカメラはあるコードで規格化されているので、利用者が記述した資源のコードを管理者側で理解することができ、アクセス要求情報３０３の一記述形態と

して用いることができる。但し、ホームネットワーク内に、例えば「ビデオカメラB」、「ビデオカメラC」というように、複数の同一規格の機器が存在する場合は、「ビデオカメラ全部」の指定では2台のビデオカメラともアクセス権設定の対象になり、「ビデオカメラ1台」の指定では、どちらか1台が対象となり、その対象を決定するアルゴリズムは特に限定しない。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図15に、アクセス権設定装置100、管理者の端末200、利用者の端末300間での動作例を示す。この例では、アクセス要求情報判定手段105が管理者の端末200にある場合として説明する。図15は、図3に示す第1の実施の形態における動作例に新たな動作1406～1408を加えたものであり、残りの1401～1405は、1001～1005に、1409～1412は1008～1011にそれぞれ対応しているため、ここでは説明を省略する。なお、1402でのアクセス要求で、利用者がアクセス権設定装置100のアクセス要求情報受付手段101へ要求を送信する場合は、ユーザIDを持たない利用者からでもアクセス要求情報受付手段101にて受け付け可能とする。

管理者の端末200からアクセス権設定装置100内のアクセス要求情報判定手段105を用いて、管理者に許可されたアクセス要求情報303は、アクセス権情報104として設定されるが、利用者はネットワークのユーザIDを持っていないため、アクセス権情報104の一部として、ユーザIDの登録が必要になる。このユーザIDは、次回資源へアクセスする際に、ユーザ認証を受けログイン可能とするために必要となる。又、アクセス制御を行う際、このユーザIDをキーにしてアクセス権の確認を行う際にも必要になる。アクセス権設定装置100内の利

用者識別子登録手段１０６は、アクセス要求情報３０３の「利用者」の情報、又は独自の方式で利用者の識別子（ユーザＩＤ）を決定し、アクセス権情報１０４の一部として登録する。この際、管理者は特にユーザＩＤの作成を意識することなく、利用者識別子登録手段１０６により自動で行われてもよいし、管理者自らユーザＩＤを決定してもよい（１４０６）。アクセス要求情報設定手段により、アクセス要求情報３０３が、アクセス権情報１０４として設定される（１４０７）。無事に設定された旨を、設定された内容、ユーザＩＤと共に（もしパスワードによってユーザ認証を行う場合は、パスワードも）、利用者の端末へ通知する（１４０８）。

上述のように構成された本発明の第４の実施の形態によれば、従来はネットワークのユーザＩＤを持たない利用者からはネットワークにログインできず、アクセス要求を行う解決策が存在していなかったが、本発明により課題が解決されることで、サービスを提供する部外者からの一時的なアクセスが考えられるホームネットワークでは、特に効果的であると言える。又、通常管理者によりユーザＩＤを決定し登録する煩雑な作業も無くなる。更に図１４に示すように、アクセス対象資源を規格化されたコードで指定ができるので、利用者は資源の識別子情報を知る必要がなくなり、管理者も利用者に識別子を伝える必要がなくプライバシーの保護に役立つといった効果がある。

（実施の形態５）

図１６は、本発明第５の実施の形態におけるネットワークシステム全体の構成を表すものである。第５の実施の形態では、利用者により指定されたアクセス要求情報に対して、管理者でも変更を可能にし、又、利用者がアクセス対象資源を種別情報で指定した場合でも、管理者が複数のアクセス対象資源の中からアクセス対象資源を決定することを目的と

する。

図１６に示す構成図は、図１１に示す第３の実施の形態の構成図に新たな構成を加えたものである。第３の実施の形態の構成とは、管理者の端末２００内に、利用者が作成したアクセス要求情報３０３を管理者の都合のいいように変更することが可能なアクセス要求情報変更手段２０５と、利用者が資源の種別情報でアクセス対象資源を指定し、該当する資源のうちどれにアクセス権を与えるか選択することが可能なアクセス対象資源選択手段２０４を備えた点が異なる。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図１７に、アクセス権設定装置１００、管理者の端末２００、利用者の端末３００間での動作例を示す。図１７は、図１５に示す第２の実施の形態における動作例に、新たな動作１５０４～１５０７を加えたものであり、残りの１５０１～１５０３は、１４０１～１４０３に、１５０８～１５１４は、１４０６～１４１２にそれぞれ対応しているため、ここでは説明を省略する。

利用者により作成されたアクセス要求情報３０３が、管理者の端末２００へ転送される。転送されてきたアクセス要求情報３０３に対して変更が必要な場合は、アクセス要求情報変更手段２０５にて変更を行う。

例として、第２の実施の形態にて説明を行った図８に示すアクセス要求情報３０３が転送された場合について説明する。管理者が人の場合は、管理者の端末２００に表示されるアクセス要求情報３０３の内容を確認し、「期間」、「アクセス対象資源」、「アクセス内容」、「条件」の変更、追加、削除などを行うことが可能である。図１８に管理者の端末２００にアクセス要求情報３０３に記述された内容の表示画面の例を示す。管理者は、画面の変更ボタンを押すことで、アクセス要求情報変更手段２０

５にて、各アクセス要求情報の内容の変更が可能になる。変更は、利用者と管理者が相互に交渉しながら行う形態でもよい（１５０４）。もし、利用者がアクセス対象資源を規格化された資源の種別情報で指定した場合、複数の資源がアクセス対象資源として設定されることになる。利用者は、利用したい資源の識別子が分からないために資源の種別情報を用いてアクセス対象資源を指定していると考えられるので、指定された種別に当てはまる全ての資源をアクセス対象資源として許可するということは、本来利用を許可する資源以外のものも許可してしまう恐れもあり、アクセス範囲を広げてしまうかもしれないという問題が発生する。そこで管理者の意思で、利用者からの利用を許可する資源の選択を行うのが望ましい。アクセス対象資源を資源の種別情報にて記述した例を挙げる。単純に「ビデオカメラ」と指定された場合は、管理者の判断で利用を許可する資源を選択する必要がある。なお許可する数量は特に限定しない。「ビデオカメラ全部」という指定の場合は、特に管理者が利用を許可する資源を選択しなくても、該当するビデオカメラを全てアクセス対象資源となる（実際には、全ての資源の識別子がアクセス権情報のアクセス対象資源として登録される）。状況に応じて利用を許可する資源を絞り込んで選択してもよい。「ビデオカメラ１台」という指定の場合は、どのビデオカメラの利用を許可するか選択しなければならない。図１９に「ビデオカメラ１台」と指定された場合の、アクセス対象資源の選択画面の例を示す。アクセス対象資源選択手段２０４により、指定された種別情報に該当する資源がピックアップされる。

管理者はこの中からアクセスを許可する資源を１つ以上選択する。ただし許可しない場合は選択しなくてもよい。なお、選択を自動化するために、あらかじめ選択される資源の優先度の指定を行ってもよいものとする（１５０５）。管理者が、アクセス権の設定を許可する判定を行う（１

５０６）。アクセス要求情報３０３が許可された場合、その情報がアクセス権設定装置１００のアクセス要求情報受付手段１０１まで返る。但し、１５０４にて要求情報の変更を行っている場合は、変更した情報が返り、更に１５０５にてアクセス対象資源の絞込み選択を行っている場合は、選択されたアクセス対象資源の識別子情報も返る（１５０７）。なお、１５０４の変更処理、１５０５の選択処理及び１５０６の判定処理の順序は特に限定しない。又、ホームネットワークの家庭の人が管理者だと仮定すると、あまり知識がないことから、１５０６のアクセス要求情報３０３の判定が、困難になるかもしれない。この場合は、１５０６の判定処理は専門家（設定代行業）に委託し、１５０４の変更処理及び１５０５の選択処理は、家庭内の人が行う、といった処理の分担を行ってもよい。すなわち、アクセス要求情報判定手段２０１、アクセス要求情報変更手段２０５及びアクセス対象資源選択手段２０４は同一端末上ではなく、分散環境としても構わないものとする。

上述のように構成された本発明の第５の実施の形態によれば、利用者により指定されるアクセス要求情報３０３を、管理者の意志で柔軟に設定できる。又、資源の識別子を知らない利用者が、資源の種別情報を用いてアクセス対象資源の指定を行った場合でも、管理者により利用を許可する資源の選択を行うことで、余計なアクセス対象資源の設定を防ぐことができる。特にホームネットワークの例のように、ネットワークの知識が乏しい管理者であっても、簡易にアクセス権の設定内容の変更及びアクセス対象資源の指定ができ、効果的であるといえる。

（実施の形態６）

図２０は、本発明第６の実施の形態におけるネットワークシステム全体の構成を表すものである。第６の実施の形態では、ネットワークのログインできない利用者のように、ネットワークに存在する資源の識別子

及びネットワークに存在する資源の種別情報を知らない場合に、これらの情報の取得を可能にすることを目的とする。

図１３に示す第４の実施の形態の構成図と異なり、図２０に示す構成では、ローカルネットワーク５００で保持している資源の識別子情報、又は種別情報の中で、外部のネットワーク向けに公開している情報と、この公開している情報を取得する公開資源情報取得手段３０５を利用者の端末３００に備えている。なお、管理者の端末２００の構成は変わっていない。

公開資源情報記憶装置に１０７に記憶されている情報の例を図２１に示す。公開資源情報記憶装置に１０７に記憶されている情報は、管理者の意志により、自由にログインできない、ユーザＩＤを持たない利用者向けに公開している情報であり、ローカルネットワーク５００内の資源の識別子及び種別の一覧情報である。この情報は、必ずしもすべての資源の情報でなく、管理者が外部のネットワークへ公開してもよいと判断した資源やそのアクセス内容に限っているものとする。言い換えると、管理者があまり外部へ公表したくない資源に関しては、公開しなくてもよいといえる。

特に図２１では、ホームネットワークの機器の例として、対象資源の項目で、ビデオカメラが２台、デジタルテレビが１台あることを表しており、それぞれ機器（資源）を一意に特定できる識別子の情報である。アクセス内容の項目では、それぞれの機器でアクセス可能な内容であることを表している。図２２は図２１の公開資源情報記憶装置に１０７に記憶されている情報を抽象化した例を示している。図２２では、機器（資源）の識別子ではなく、種別の情報であるので、仮にビデオカメラが複数台存在する場合でも、１通りの表現で表されることになる。なお、この公開資源情報記憶装置に１０７に記憶されている情報は、管理者及び

利用者からの通信が可能であれば、特に存在する場所は限定しない。

通常、管理者からの告知がない限り、資源の存在を知ることが困難なネットワークにログインできない利用者でも、利用者の端末３００内の公開資源情報取得手段３０５を用いて公開資源情報記憶装置に１０７に記憶されている情報を取得することができる。取得した公開資源情報記憶装置に１０７に記憶されている情報は、アクセス要求情報３０３として、利用したい資源やアクセス内容を指定するときに用いることができる。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図２３に、アクセス権設定装置１００、管理者の端末２００、利用者の端末３００間での動作例を示す。この例では、図１６に示す管理者の端末２００を利用するものとして説明する。図１８は、図１３に示す第４の実施の形態における動作例に新たな動作１６０１、１６０２を加えたものであり、残りの１６０３～１６１５は、１５０２～１５１４に対応しているため、ここでは説明を省略する。

ネットワークへログインできない利用者、又はネットワークの資源の情報を知らない利用者が、利用者の端末３００内の公開資源情報取得手段３０５を用いて、公開資源情報記憶装置１０７から資源の識別子、又は種別情報などの情報を取得する。もし、公開資源情報記憶装置１０７がアクセス権設定装置１００内に存在する場合でも、ネットワークへログインするために必要なユーザＩＤを持たない利用者から、ある通信規約（プロトコル）を用いてアクセスできるものとする（１６０１）。取得した公開資源情報記憶装置１０７に記憶されている情報を基にアクセス対象資源を指定ができるので、結果として利用者の端末３００内のアクセス要求情報作成手段３０１を用いて、アクセス要求情報３０３を作成

することが可能となる（１６０２）。

上述のように構成された本発明の第６の実施の形態によれば、資源の識別子を知らない場合でも、オンラインで即時に情報を取得することができる。特にネットワークのユーザＩＤを持たずログインできない利用者は、あらかじめ資源の識別子を知らないことがほとんどであると考えられる。この点からも、識別子情報及び種別情報の取得は有効な手段であるといえる。

（実施の形態７）

図２４は、本発明第７の実施の形態におけるネットワークシステム全体の構成を表すものである。第７の実施の形態では、利用者が作成したアクセス要求情報３０３が信頼のおけるものかの確認と、管理者である人間に知られないように、不正にアクセス権の設定を行わせないようにすることが目的となる。

図２０に示す第６の実施の形態の構成図と異なり、図２４に示す構成では、アクセス権設定装置１００内に、利用者が作成したアクセス要求情報３０３が、信頼できる情報かどうかの認証を行うアクセス要求情報認証手段１０８と、利用者が作成したアクセス要求情報に記述された内容を、人が視覚的に理解し易い自然言語へと変換し表示情報を作成する表示情報作成手段１０９を備えている。なお、管理者の端末２００及び利用者の端末３００の構成は変わっていない。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

まず第１に、アクセス要求情報３０３が信頼のおける情報かを認証する仕組みを説明する。

例としてホームネットワークに導入するサービスを考えた場合、第３者により作成されているものであれば、すべてのサービスが信頼できる

訳ではなく、中には不正行為を働くサービスも存在するかもしれない。信頼できるサービスかの判断を行う手段として、デジタル署名の仕組みがあり、本実施の形態では、この仕組みを利用し、サービスの信頼性を確認する。

以下、例として公開鍵暗号方式を利用したデジタル署名の基づく、ユーザ認証について説明する。デジタル署名の仕組みをアクセス要求情報３０３に利用すると、不正利用者が名前を偽る「なりすましの防止」、不正利用者によるアクセス要求情報３０３の書き換えなどの「改ざんの防止」、又は、利用者が公的な認証機関によって認証された事実による「信頼度の向上」などを図ることができる。

まず「なりすましの防止」の説明を行う。利用者が作成したデジタル署名を施したアクセス要求情報３０３を不正利用者が何らかの手段で入手し、これを送信した場合を考える。通常管理者が入手した利用者の公開鍵を利用して、間違いなく利用者から送信されたものかのユーザ認証を行う。しかし、この場合、不正利用者はユーザ認証を行う際に必要な、利用者の公開鍵のペアとなる秘密鍵を持っていないため、ユーザ認証が失敗する。従って、なりすましを防止することできる。

次に「改ざんの防止」の説明を行う。利用者が作成したデジタル署名を施したアクセス要求情報３０３を不正利用者が何らかの手段で入手し、これを改ざんを行った場合を考える。本当は利用者の秘密鍵で暗号化しなければならないところ、不正利用者は、この秘密鍵を持っていないため、別の秘密鍵で暗号化するしかない。しかし、管理者は利用者の公開鍵にて復号化を行い、うまくアクセス要求情報３０３が復号化できず、不正に改ざんされたことが分かる。従って、改ざんを防止することができる。

最後に「利用者の信頼度の向上」の説明を行う。信頼のできる第３者

認証機関であるＣＡ（Certification Authority：認証局）を利用する例である。なお、ＣＡは公正、中立な立場であり、絶対的に信頼できる機関であることが前提となる。利用者は、自分専用の公開鍵、秘密鍵のペアを自ら作成するかＣＡで作成してもらい、それをＣＡへ登録申請する。このとき、ＣＡにより利用者の身元照会が行わる。ＣＡは利用者の身元照会により登録を許可すると、利用者の公開鍵をＣＡのデータベースに登録し保管する。そして、登録者の情報をＣＡの秘密鍵で暗号化した証明書を利用者に渡す。すなわち、この証明書がＣＡの公開鍵で復号化できれば、ＣＡに認定された信頼のおける利用者と判断することができる。

第２に、管理者である人間に知られないように、不正にアクセス権の設定を行わせないようにする仕組みを説明する。

まず課題を分かり易く説明する。例として第３者が作成したソフトを、自分のコンピュータで実行する場合を考える。人に見える動作としては、画面に表示されている映像や音があるが、これ以外の人に見えないところでは、ソフトが何を行っているか分からない。つまり、人に見える範囲では特に問題ないような動きをし、人に見えないところで気付かれないように、不正にアクセス権の設定を行うようなソフトを作成することが可能である。本発明の内容で具体的な例として、悪意のある利用者が、特に問題のない表現で記述された人間が理解し易い自然言語情報と、不正を働く記述がされた人工言語情報とでアクセス要求情報３０３を作成し、管理者に不正であることを気付かせずにアクセス要求情報３０３を許可させ、人工言語で記述された不正な内容でアクセス権の設定を行えることが挙げられる。

利用者が不正に作成したアクセス要求情報３０３の例を図２５に示す。図２５では例として、アクセス要求情報３０３に人工言語、自然言語を記述しており、人工言語をＸＭＬにて記述している。ここで問題になる

のは、機械が理解できる人工言語では、資源を利用できる「期間」が「2000/1/1～2000/2/29」、「アクセス対象資源」が「0x0004（=ビデオカメラ）」（図２６の変換テーブル記載のコードの定義を参照）、「アクセス内容」が「0x1020（=すべての動作）」となっているが、一方、管理者である人が理解できる自然言語では、それぞれ「1999/12/1～2000/5/31」、「ビデオカメラ」、「映像取得」と異なった内容の記述がされている。本来、人工言語と自然言語は同じ意味の記述をしなければならないが、この例だと、利用者が管理者を騙して、不正なアクセス権の設定を行う可能性があると言える。

一旦不正にアクセス権が設定されると、資源への不正アクセスが起こる恐れがあり、セキュリティ上問題になる。第２の実施の形態などで説明したホームネットワークで導入するサービスの例だと、当然すべてが信頼できるサービスとは言えず、中には不正な設定を行い、家庭の機器へ不正にアクセスしたり、家庭の情報を盗み出すサービスが存在する可能性もあり、これを解決する仕組みが必要となる。なお、管理者が機械の場合は、もともと自然言語を理解することができないため、この仕組みは適用できない。

このような不正行為を防止するためには、必ずしも信頼できないので利用者が作成した自然言語情報を利用せずに、信頼できるアクセス権設定装置の一手段が自然言語情報を作成する方式を考案する。利用者によって作成された人工言語情報を含むアクセス要求情報３０３を基に、人工言語と自然言語を対応させて変換を行い、表示情報作成手段１０９にて、自然言語形式の表示情報を作成する。

人工言語から自然言語へ翻訳する際の対応を取った変換テーブルの例を図２６に示す。

図２６には、第２の実施の形態にて説明した図８に示す「アクセス対

象資源」、「アクセス内容」、「条件」などの各人工言語に対応した自然言語が記載されている。例えば、利用者により「対象資源」が「0x0004」で「アクセス内容」が「0x1020」と指定された場合、アクセス権設定装置１００の表示情報作成手段１０９にて、「ビデオカメラのすべての動作」というように、文字列による自然言語への変換を可能にする。但し、この人工言語はある規約により定められたもので、利用者、管理者、双方で既知であることが前提となる。なお、図２６には例として自然言語を文字列の形で表しているが、他にも画像、音声などがあり、どの形式を使用してもよい。又、図２６の変換テーブルを用いた自然言語の作成アルゴリズムは一例であり、作成方式は特に限定しない。

図２７に、アクセス権設定装置１００、管理者の端末２００、利用者の端末３００間での動作例を示す。この例では、図１６に示す管理者の端末２００を利用するものとして説明する。図２７は、図２３に示す第６の実施の形態における動作例に、新たな動作１７０４～１７０６を加えたものであり、残りの１７０１～１７０３は、１６０１～１６０３に、１７０６～１７１７は、１６０４～１６１５にそれぞれ対応しているため、ここでは説明を省略する。

アクセス要求情報受付手段１０１が、暗号化されたアクセス要求情報３０３とそれに付随するＣＡが発行した証明書、又はデジタル署名を受け付け、アクセス要求情報認証手段１０８へアクセス要求情報３０３の認証を依頼する。復号化に必要なＣＡ、又は利用者の公開鍵は、アクセス要求情報３０３と共に送信されるか、又はネットワーク上のアクセス可能なＤＢ（データベース）から取得できる。該当する公開鍵で暗号化されているアクセス要求情報３０３、又は証明書を復号化し、利用者のユーザ認証を行うと共に、公開鍵、秘密鍵を、用いて認証を行う（１７０４）。認証が通った場合、利用者により人工言語のみで記述されたアク

セス要求情報３０３は、表示情報作成手段１０９にて人工言語を読み取られ、アクセス要求情報３０３を適切な自然言語へと変換され、結果として人間が理解し易い表示情報が作成される（１７０５）。表示情報作成手段１０９にて作成された表示情報が、アクセス要求情報転送手段１０２により、管理者の端末２００へ転送される（１７０６）。

図２８に、第７の実施の形態のアクセス要求情報３０３の認証手段及びアクセス要求情報３０３から自然言語を作成する手段を加えたフローチャートを示す。

利用者が作成したアクセス要求情報３０３を受け付ける（１８０１）。アクセス要求情報３０３のデジタル署名を参照して信頼できる情報かの認証を行う（１８０２）。認証されない場合は、アクセス要求情報３０３は設定されず（１８０８）、不許可の結果が利用者へ通知される（１８０９）。認証された場合は、表示情報作成手段１０９にて、アクセス要求情報の内容を自然言語に変換し、管理者に提示するための表示情報を作成する（１８０３）。以降の１８０４～１８０７は、図６に示す１１０２～１１０５と同じフローなので、ここでは説明を省略する。

上述のように構成された本発明の第７の実施の形態によれば、デジタル署名を利用した認証の仕組みを利用することで、利用者が信頼でき、更にアクセス要求情報３０３も信頼できるものか確認を行うことが可能である。特に多種多様なサービスが考えられるホームネットワークでは、ネットワーク上に散在している信頼できないサービスの存在も懸念されるので、このような認証の仕組みを利用することで、不正なサービスの導入を防ぐ効果がある。

又、利用者が用意する管理者へアクセス要求情報の内容を理解してもらうための自然言語情報で、実際の設定内容を誤魔化される恐れがあるという課題に対し、信頼できるアクセス権設定装置が、人間が理解でき

る自然言語を用いた表示情報を作成する機能を持つことで、利用者が指定した内容を忠実に管理者へ伝えることができ、利用者による不正なアクセス権の設定を防ぐことが可能となり、セキュリティ向上の効果がある。

（実施の形態８）

図２９は、本発明第８の実施の形態におけるネットワークシステム全体の構成を表すものである。第８の実施の形態では、管理者の端末にて行っていた、アクセス要求情報の判定、対象資源の絞込み選択、アクセス要求情報記述の内容の変更を、携帯端末にて行わせることが目的となる。

図２４に示す第７の実施の形態の構成図と異なり、図２９に示す構成では、アクセス権設定装置１００内に、管理者がアクセス権の設定を行うために用いる携帯端末６００と、携帯端末６００へアクセス要求情報３０３を転送する携帯端末用要求情報転送手段１１０と、携帯端末６００にて、アクセス要求情報３０３をアクセス権情報１０４として設定するかの可否判定を行う携帯端末用要求情報判定手段１１１と、携帯端末６００にて、複数のアクセスの対象となる資源の候補の中から絞込み選択を行う携帯端末用対象資源選択手段１１２と、携帯端末６００にて、アクセス要求情報３０３に記述された内容の変更を行う携帯端末用要求情報変更手段１１３を備えている。なお、ここで記述している携帯端末６００とは、人間により比較的自由に持ち運びができ、且つ、ネットワークとの接続手段を備えているものと仮定する。又、管理者の端末２００及び利用者の端末３００の構成は変わっていない。

上述の１１０、１１１、１１２、１１３、の各手段は、図１６に示す管理者の端末２００内にある２０２、２０１、２０４、２０５の各手段を携帯端末用に拡張したもので、目的は同じものと考えてよい。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図３０に、アクセス権設定装置１００、携帯端末６００間での動作例を示す。図３０では、第７の実施の形態以前のアクセス要求情報３０３を受け取る処理及び取得する処理と、管理者からの判定結果を受けてのアクセス権の設定処理について、動作が同じであるため省略しており、アクセス権設定装置１００と携帯端末６００間の動作についてのみ説明する。

アクセス要求情報３０３を受け付けた、又は取得したアクセス権設定装置１００は、携帯端末用要求情報転送手段１１０により携帯端末６００へ転送する。転送された画面の例は図１８の通りである（１９０１）。管理者が携帯端末６００の画面上で、図１８に示されるような変更ボタンを押すことで、アクセス要求情報３０３の内容の変更要求を行う（１９０２）。この要求を受け取った携帯端末用要求情報変更手段１１３は、管理者の指定した変更画面を携帯端末６００へ送信し表示させる（１９０３）。受け取った管理者は、変更画面にてアクセス要求情報３０３の記述内容の変更を行う（１９０４）。管理者が指定した変更内容を受け取った携帯端末用要求情報変更手段１１３は、その変更内容を反映させた変更結果を携帯端末６００へ送信し表示させる(１９０５)。次に管理者は、アクセス対象資源の候補が複数ある場合に、アクセス対象資源の絞込みのために対象資源の選択要求を行う。この選択は、第４の実施の形態で説明した通り、利用者がアクセス要求情報３０３のアクセス対象資源の項目に資源の種別を記述した場合に起こり得る処理である（１９０６）。この要求を受け取った携帯端末用対象資源選択手段１１２は、管理者の指定した図１９に示されるような資源の選択画面を携帯端末６００へ送信し表示させる。（１９０７）。受け取った管理者は、選択画面にてアク

セス対象資源の候補の中から、実際にアクセス権の設定を行う資源の選択を行う（１９０８）。管理者が指定した選択資源の情報を受け取った携帯端末用対象資源選択手段１１２は、その選択資源を反映させた選択結果を携帯端末６００へ送信し表示させる（１９０９）。管理者が、アクセス権の設定を許可する判定を行う（１９１０）。アクセス要求情報３０３が許可された場合、その情報が携帯端末用要求情報判定手段１１１まで返る（１９１１）。なお、１９０２～１９０５の変更処理、１９０６～１９０９の選択処理及び１９１０、１９１１の判定処理の順序は特に限定しない。

上述のように構成された本発明の第８の実施の形態によれば、アクセス権設定装置１００から携帯端末６００へアクセス要求情報３０３の内容を転送し、アクセス要求情報３０３の許可判定、アクセス対象資源の選択、アクセス要求情報３０３に記述された内容の変更といった処理が行えることにより、管理者が外出している場合でも、携帯端末６００を持って外出している場合などでも、管理者の端末２００で行える処理を携帯端末６００で行うことができる。利用者の端末に常にいる必要がなく、又アクセス要求情報３０３が送信されたり、取得した場合でも、即時に携帯端末まで転送されるので、リアルタイムな設定が可能になる。

産業上の利用可能性

以上のように本発明によれば、第１に、利用者による、アクセス権の設定の要求と設定内容の指定ができることにより、ネットワークの知識のない管理者でも簡易にアクセス権の設定が可能になると共に、利用者も希望通りのアクセス権の設定が可能となる。又、ホームネットワークにサービスを導入するような、頻繁にアクセス権の設定が伴うネットワークでは、アクセス権の設定が簡易なことから特に有効である。

第２に、利用者側からアクセス要求情報を取得できることにより、管理者が希望するときに簡易にアクセス権の設定を行うことができ、更に、利用者から一方的にアクセス要求情報を送信されることもなくなるので、不正アクセスの危険度を低くする効果がある。

第３に、アクセス要求情報に記述された内容をアクセス権情報として設定してもよいかの可否判定を、機械により自動で行えることにより、通常人間が行っていた煩雑な作業を無くすことができ、人間がいない場合でもアクセス権の設定が可能になる効果がある。

第４に、受け取ったアクセス要求情報から、ユーザＩＤを発行し、アクセス権情報の一部として登録できることにより、ネットワークのユーザＩＤを持たずログインできない利用者からも、アクセス要求情報を受け付けることが可能になる。

第５に、利用者が作成するアクセス要求情報に記述するアクセス対象資源を、抽象化した種別の情報で指定することを可能にしたことにより、利用者はあらかじめ資源の存在や識別子を知っておく必要がなくなり、又管理者は、自分が管理する機密資源の情報を利用者へ知らせる必要がなくなるという効果がある。

第６に、利用者が種別情報でアクセス要求情報に記述するアクセス対象資源を指定した場合に、複数の対象資源の候補の中から、管理者が自由にアクセスを許可する資源を選択できることにより、管理者の好みに応じて数を絞り込むことができ、余分にアクセス権の設定をしなくてもよいという効果がある。

第７に、利用者が指定したアクセス要求情報に対し、管理者がその内容の変更ができることにより、一方的に指定されるばかりではなく、管理者の意思を尊重した柔軟な設定や、利用者との交渉をすることで、より的確な設定が可能という効果がある。

第８に、管理者が外部のネットワークに公開した資源の識別子及び種別の情報を、利用者が取得できることにより、資源の情報を知らない利用者でも、アクセス要求情報にアクセス対象資源を記述することができ、アクセス権の設定要求をすることが可能になる。

第９に、利用者が作成したアクセス要求情報の内容を、人間である管理者が理解し易い自然言語へ忠実に変換し、管理者の端末で表示する情報を作成することにより、利用者が管理者に嘘をついて、不正にアクセス権の設定を行わせるのを防ぐ効果がある。

第１０に、デジタル署名を利用したアクセス要求情報の認証を行うことにより、不正行為を働こうとしている利用者から、他人のアクセス要求情報を使う成りすましの防止、他人のアクセス要求情報の書き換え防止、並びにアクセス要求情報の信頼性の確認を行うことができる。

第１１に、管理者が利用する携帯端末にアクセス要求情報に記述された内容を転送させ、更にアクセス権情報として設定するかの判定も可能にしたことにより、管理者が遠隔地にいる場合や、アクセス要求情報を受け付け、即時に対応したい場合などに効果がある。

第１２に、第６の効果に記載した内容を、管理者が利用する携帯端末でも奏することができる。

第１３に、第７の効果に記載した内容を、管理者が利用する携帯端末でも奏することができる。

請 求 の 範 囲

1. アクセス権の設定により利用の制限が可能な資源に対し、前記資源の利用を制限するためのアクセス権情報の設定を行うことができるアクセス権設定装置において、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報を受け付けるアクセス要求情報受付手段と、

前記アクセス要求情報受付手段により受け付けた前記アクセス要求情報の内容の判定を行うアクセス要求情報判定手段と、

前記アクセス要求情報判定手段により判定した前記アクセス要求情報の内容を、前記アクセス権情報として設定を行うアクセス要求情報設定手段を備えたことを特徴とするアクセス権設定装置。

2. アクセス権の設定により利用の制限が可能な資源に対し、前記資源の利用を制限するためのアクセス権情報の設定を行うことができるアクセス権設定装置において、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報の取得を依頼するアクセス要求情報取得依頼手段と、

前記アクセス要求情報取得依頼手段により指定された前記アクセス要求情報の取得を行うアクセス要求情報受付手段と、

前記アクセス要求情報受付手段により取得した前記アクセス要求情報の内容の可否判定を行うアクセス要求情報判定手段と、

前記アクセス要求情報判定手段により判定した前記アクセス要求情報の内容を、前記アクセス権情報として設定を行うアクセス要求情報設定手段を備えたことを特徴とするアクセス権設定装置。

3．　アクセス権の設定により利用の制限が可能な資源に対し、前記資源の利用を制限するためのアクセス権情報の設定を行うことができるアクセス権設定装置であって、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報を受け付けるアクセス要求情報受付手段と、

前記アクセス要求情報受付手段により受け付けた前記アクセス要求情報の内容の判定を行うアクセス要求情報判定手段と、

前記アクセス要求情報判定手段により判定した前記アクセス要求情報の内容を、前記アクセス権情報として設定を行うアクセス要求情報設定手段を備えたアクセス権設定装置とネットワークにて接続された管理者端末において、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報の取得を依頼するアクセス要求情報取得依頼手段と、

前記アクセス権設定装置より前記アクセス要求情報を受け取り、前記アクセス要求情報の内容の可否判定を行うアクセス要求情報判定手段と、

自動的に可否判定を行うアクセス要求情報自動判定手段を備えたことを特徴とする管理者端末。

4．　アクセス権の設定により利用の制限が可能な資源に対し、前記資源の利用を制限するためのアクセス権情報の設定を行うことができるアクセス権設定装置であって、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報の取得を依頼するアクセス要求情報取得依頼手段と、

前記アクセス要求情報取得依頼手段により指定された前記アクセス要求情報の取得を行うアクセス要求情報受付手段と、

前記アクセス要求情報受付手段により取得した前記アクセス要求情報

の内容の可否判定を行うアクセス要求情報判定手段と、

前記アクセス要求情報判定手段により判定した前記アクセス要求情報の内容を、前記アクセス権情報として設定を行うアクセス要求情報設定手段を備えたアクセス権設定装置とネットワークにて接続された管理者端末において、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報の取得を依頼するアクセス要求情報取得依頼手段と、

前記アクセス権設定装置より前記アクセス要求情報を受け取り、前記アクセス要求情報の内容の可否判定を行うアクセス要求情報判定手段と、

自動的に可否判定を行うアクセス要求情報自動判定手段を備えたことを特徴とする管理者端末。

5. 請求項１又は２に記載のアクセス権設定装置において、

前記資源へアクセスするための前記アクセス権設定装置への接続ができない利用者向けに、前記接続を可能にするためのユーザ認証を行うのに必要な利用者を一意に特定する識別子を発行し、前記アクセス権情報の一部として登録する利用者識別子登録手段を備えたことを特徴とするアクセス権設定装置。

6. 請求項１、２及び５のいずれか１つに記載のアクセス権設定装置において、

前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源の指定について、前記資源を一意に特定する識別子ではなく、前記資源の種別の識別子で指定された前記アクセス要求情報を受け付けることが可能なアクセス要求情報受付手段を備えたことを特徴とするアクセス権設定装置。

7．　　請求項３又は４記載の管理者端末において、

前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源を、前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源の指定について、前記資源を一意に特定する識別子ではなく、前記資源の種別の識別子にて指定したときに、該当する前記資源が複数存在する場合、前記管理者が前記複数の資源の中から利用の対象となる前記資源を選択できるアクセス対象資源選択手段を備えたことを特徴とする管理者端末。

8．　　請求項３、４及び７のいずれか１つに記載の管理者端末において、

前記アクセス権設定装置より受け取った前記アクセス要求情報に記述された内容の変更が可能な、アクセス要求情報変更手段を備えたことを特徴とする管理者端末。

9．　　請求項１、２、５及び６のいずれか１つに記載のアクセス権設定装置において、

前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源の指定について、前記資源を一意に特定する識別子ではなく、前記資源の種別の識別子の情報の内、前記資源のアクセス元に対して公開する情報として記憶可能な公開資源情報記憶装置を備えたことを特徴とするアクセス権設定装置。

１０．　　請求項１、２、５、６及び９のいずれか１つに記載のアクセス権設定装置において、

前記アクセス要求情報を正確に前記管理者へ通知するために、前記アクセス要求情報に記述された内容を、視覚的に理解し易い自然言語へ変換することが可能な表示情報作成手段を備えたことを特徴とするアクセス権設定装置。

１１．　請求項１、２、５、６、９及び１０のいずれか１つに記載のアクセス権設定装置において、

前記アクセス要求情報が、改ざん、又は成りすましに代表される不正行為によって作成されていないこと確認するため、前記アクセス要求情報の認証を行うアクセス要求情報認証手段を備えたことを特徴とするアクセス権設定装置。

１２．　請求項１、２、５、６、９、１０及び１１のいずれか１つに記載のアクセス権設定装置において、

前記アクセス要求情報に記述された内容を遠隔地で把握するために携帯端末へ転送する携帯端末用要求情報転送手段と、

前記アクセス要求情報の可否判定を前記携帯端末から行うための携帯端末用要求情報判定手段を備えたことを特徴とするアクセス権設定装置。

１３．　請求項１２に記載のアクセス権設定装置において、

前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源を、前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源の指定について、前記資源を一意に特定する識別子ではなく、前記資源の種別の識別子にて指定したときに、該当する前記資源が複数存在する場合、前記管理者が前記複数の資源の中から利用の対象となる前記資源を選択できるアクセス対象資源選択手段にて行う前記アクセス対

象の資源の選択を、前記携帯端末から行うための携帯端末用対象資源選択手段を備えたことを特徴とするアクセス権設定装置。

１４．　請求項１２又は１３に記載のアクセス権設定装置において、前記アクセス要求情報に記述された内容の変更を、前記携帯端末から行うための携帯端末用要求情報変更手段を備えたことを特徴とするアクセス権設定装置。

図1

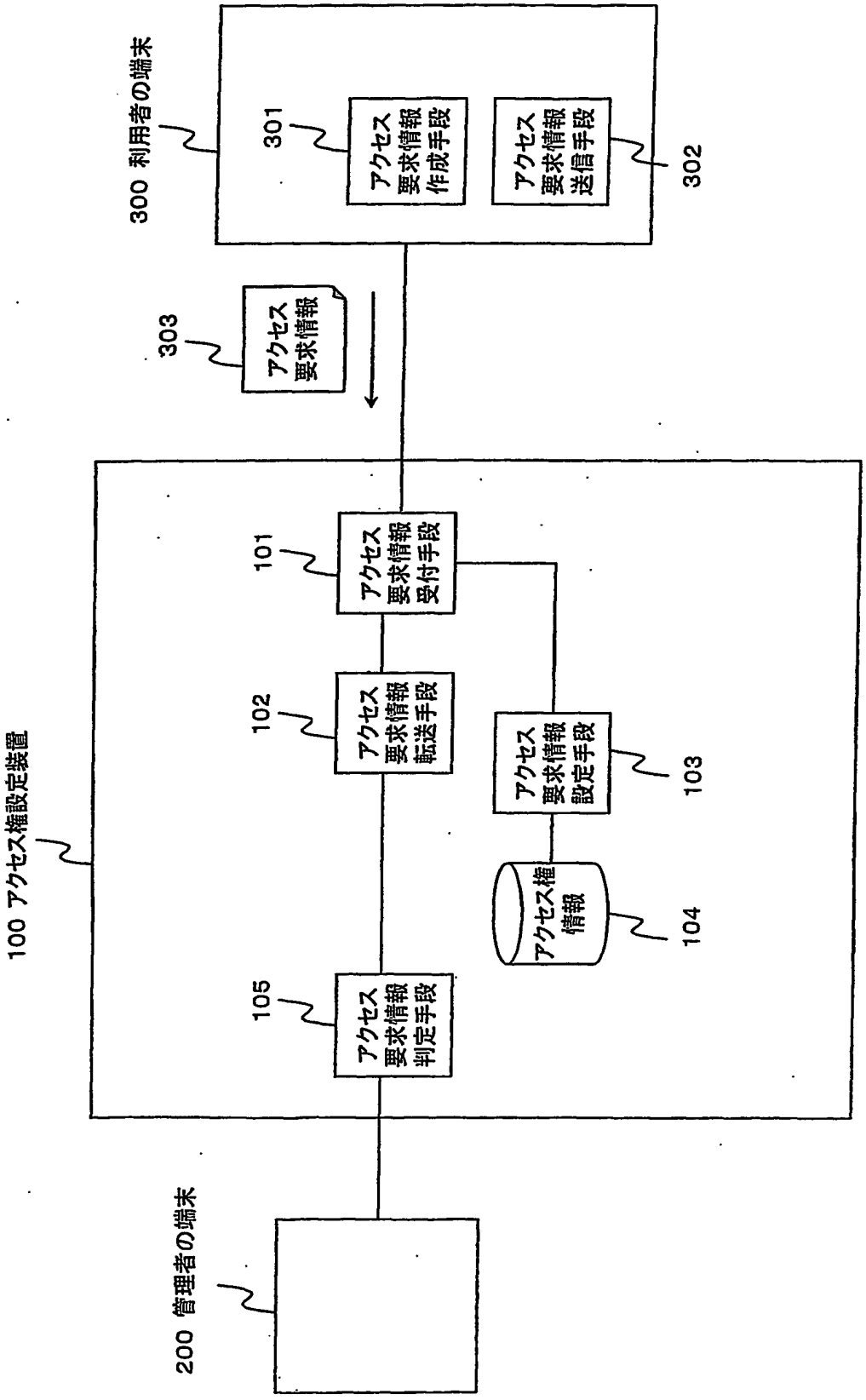

300 利用者の端末
301
アクセス要求情報作成手段
アクセス要求情報送信手段
302
303
アクセス要求情報
100 アクセス権設定装置
101
アクセス要求情報受付手段
102
アクセス要求情報転送手段
アクセス要求情報設定手段
103
アクセス権情報
104
105
アクセス要求情報判定手段
200 管理者の端末

図 2

アクセス要求情報の例

利用者：	利用者Ａ
利用端末：	111. 222. 111. 222
期間 ：	2000/1/25 ～ 2000/2/29
アクセス対象資源 ：	ファイルB
アクセス内容：	読み出し、書き込み

図 3

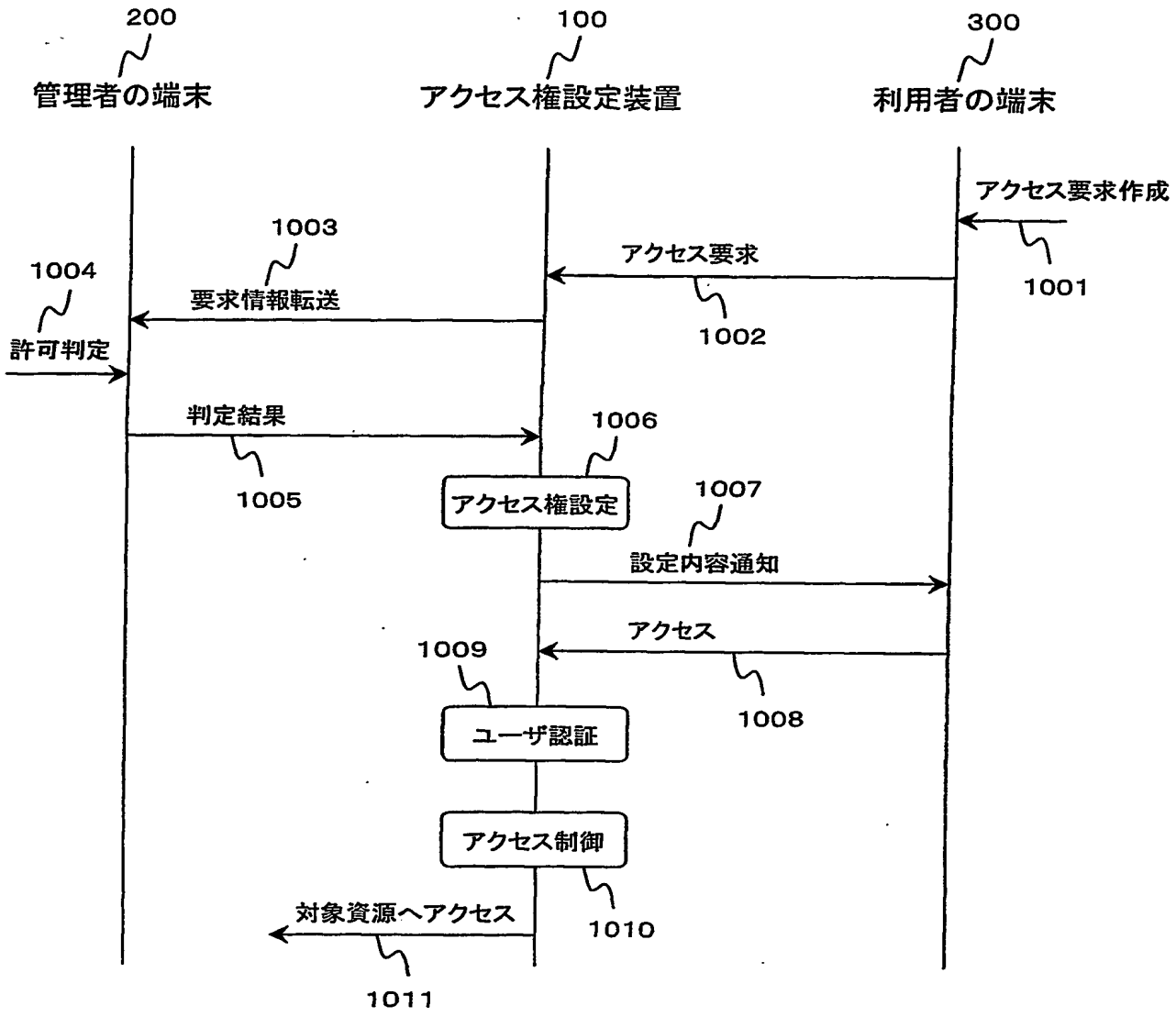

200
管理者の端末
100
アクセス権設定装置
300
利用者の端末
アクセス要求作成
1001
アクセス要求
1002
1003
要求情報転送
1004
許可判定
判定結果
1005
1006
アクセス権設定
1007
設定内容通知
アクセス
1008
1009
ユーザ認証
アクセス制御
1010
対象資源へアクセス
1011

図4

判定画面の例

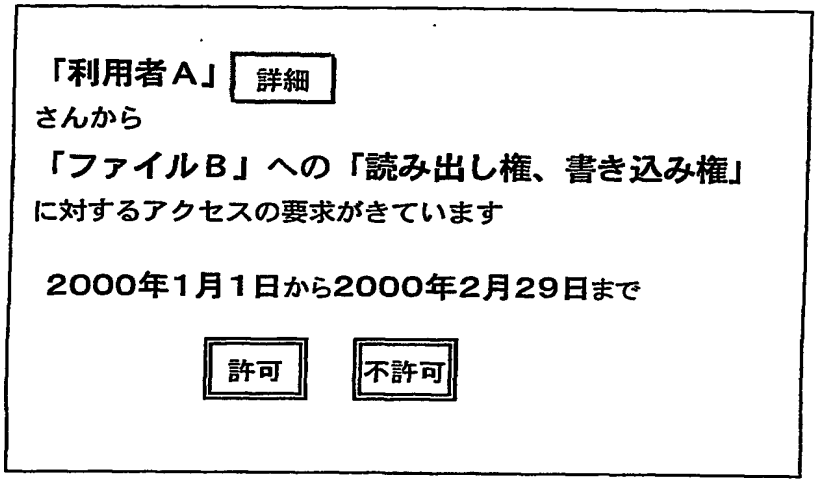


図5

利用者への通知画面の例

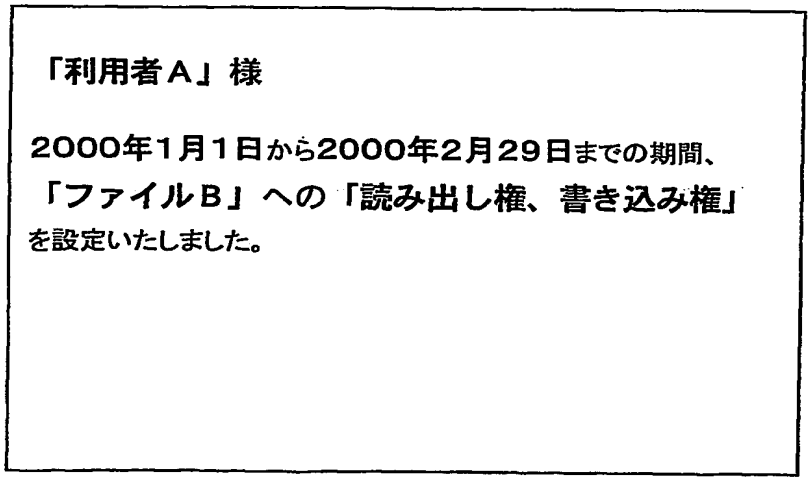


図 6

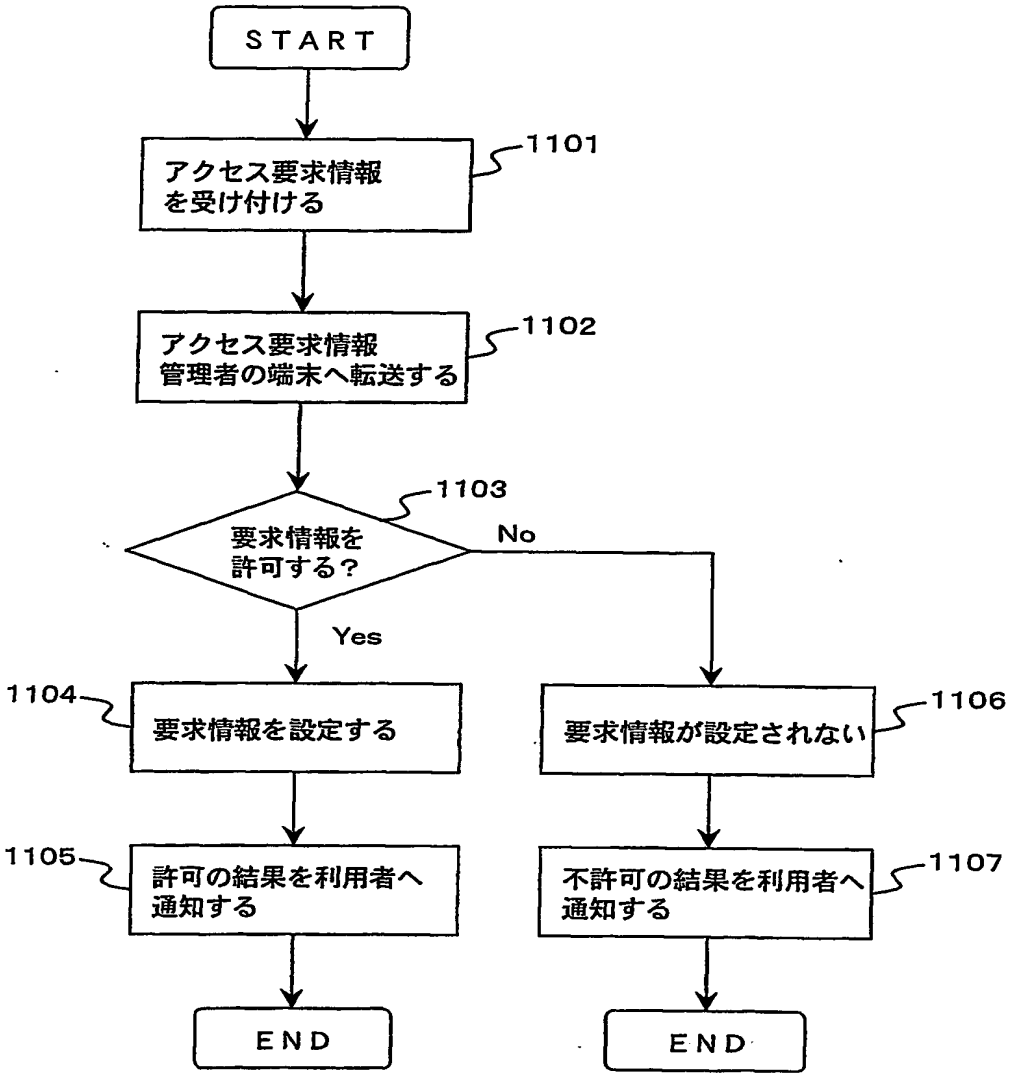

START
アクセス要求情報を受け付ける
1101
アクセス要求情報管理者の端末へ転送する
1102
要求情報を許可する？
1103
No
Yes
1104
要求情報を設定する
1105
許可の結果を利用者へ通知する
END
要求情報が設定されない
1106
不許可の結果を利用者へ通知する
1107
END

図7

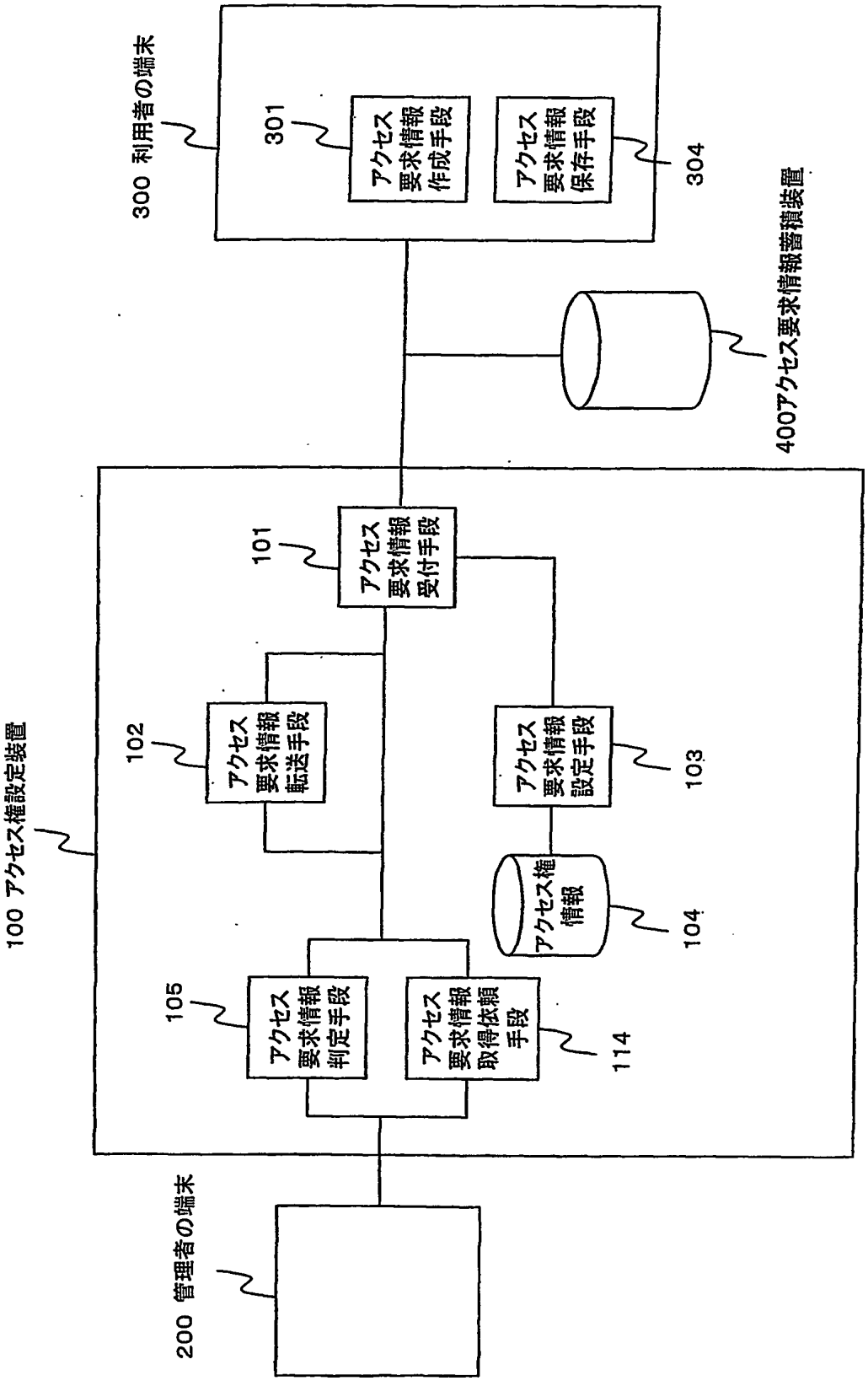

300 利用者の端末
301
アクセス要求情報作成手段
アクセス要求情報保存手段
304
400アクセス要求情報蓄積装置
100 アクセス権設定装置
101
アクセス要求情報受付手段
102
アクセス要求情報転送手段
103
アクセス要求情報設定手段
アクセス権情報
104
105
アクセス要求情報判定手段
アクセス要求情報取得依頼手段
114
200 管理者の端末

図8

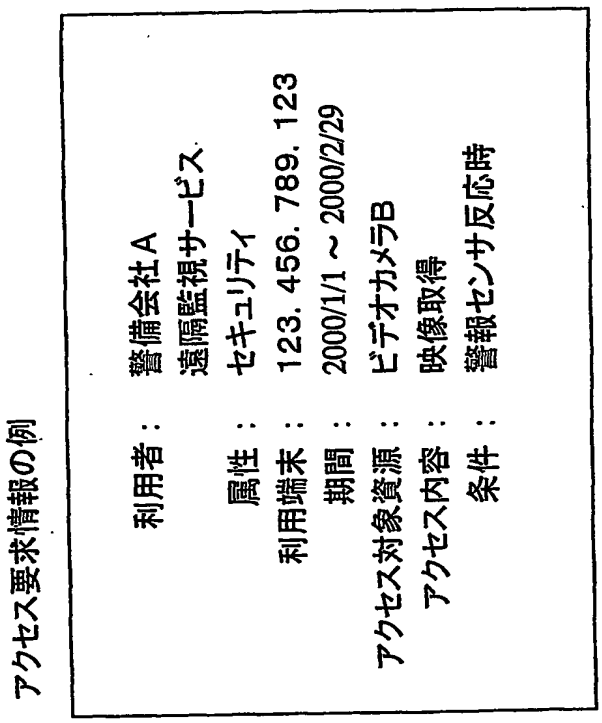

アクセス要求情報の例
利用者：警備会社A
遠隔監視サービス
属性：セキュリティ
利用端末：123. 456. 789. 123
期間：2000/1/1 ～ 2000/2/29
アクセス対象資源：ビデオカメラB
アクセス内容：映像取得
条件：警報センサ反応時

図9

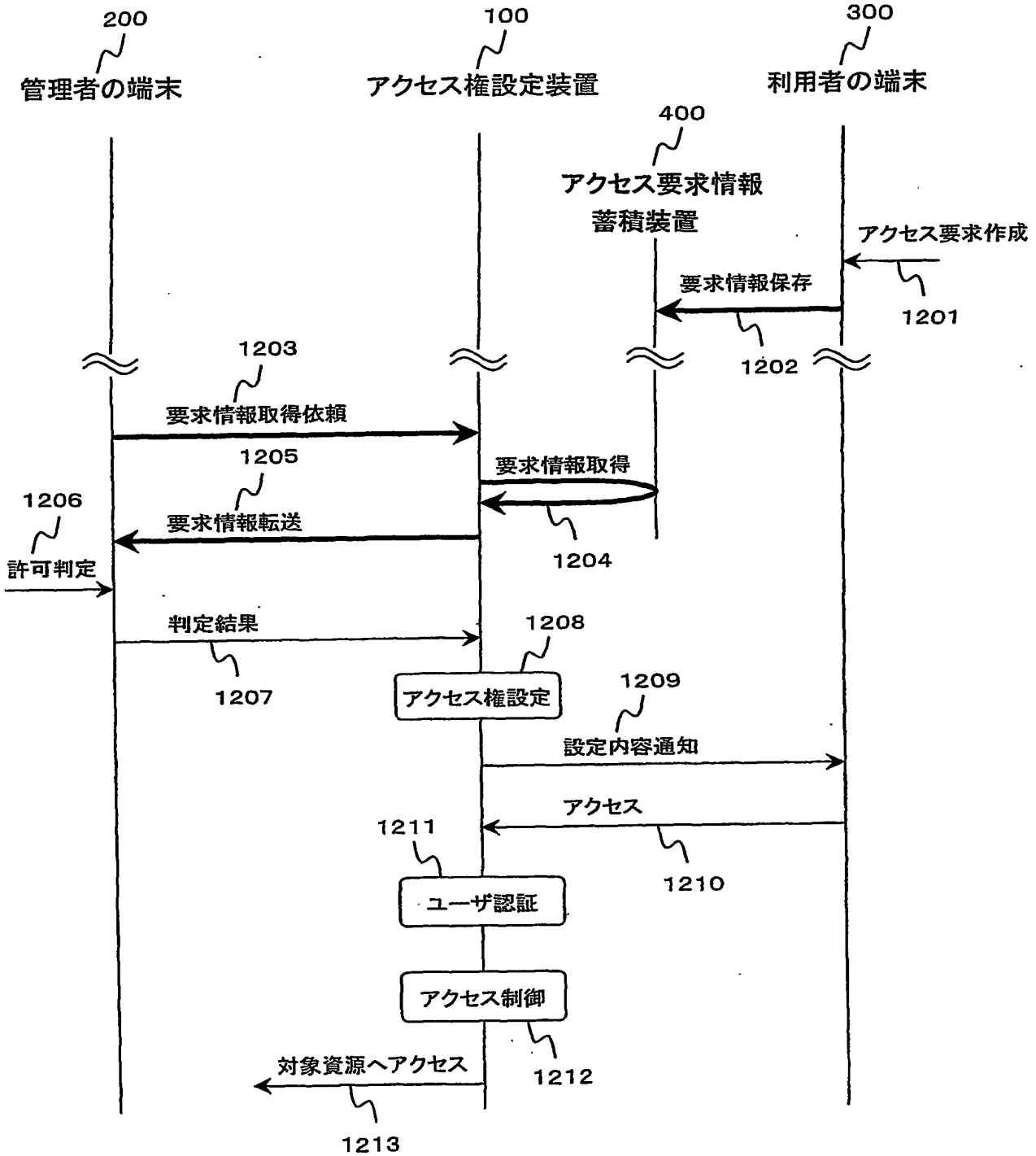

200
管理者の端末
100
アクセス権設定装置
300
利用者の端末
400
アクセス要求情報
蓄積装置
アクセス要求作成
1201
要求情報保存
1202
1203
要求情報取得依頼
1205
要求情報取得
1204
1206
要求情報転送
許可判定
判定結果
1207
1208
アクセス権設定
1209
設定内容通知
アクセス
1210
1211
ユーザ認証
アクセス制御
1212
対象資源へアクセス
1213

図10

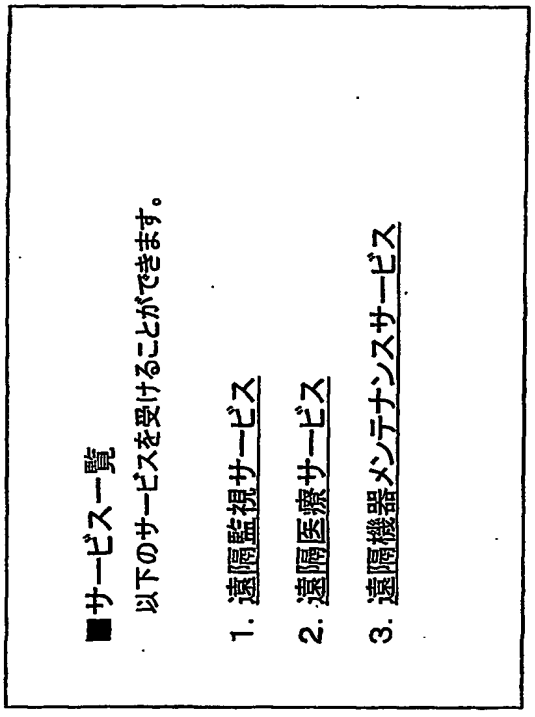

サービス一覧画面の例
■サービス一覧
以下のサービスを受けることができます。
1. 遠隔監視サービス
2. 遠隔医療サービス
3. 遠隔機器メンテナンスサービス

図11

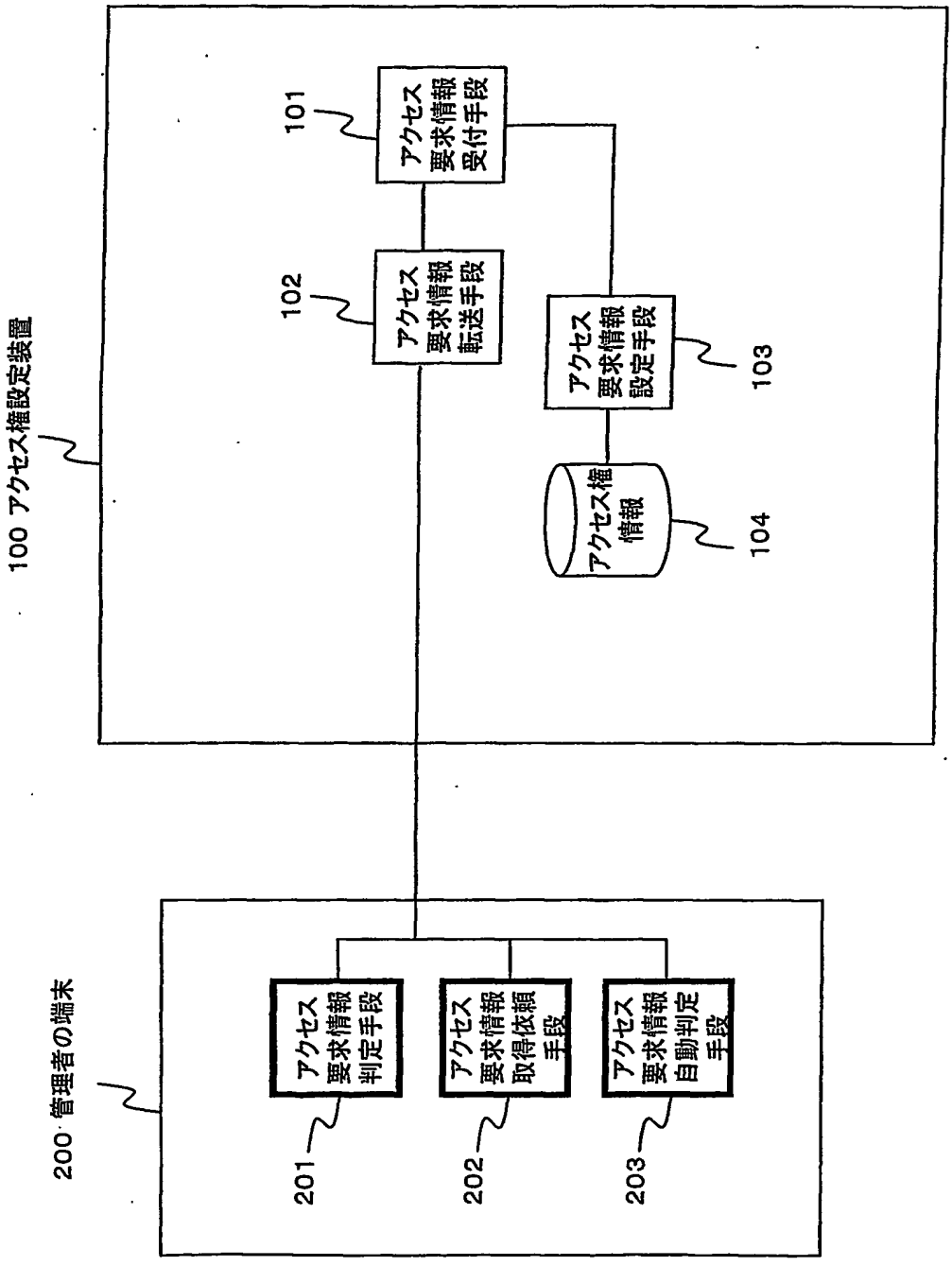

100 アクセス権設定装置
101
アクセス要求情報受付手段
102
アクセス要求情報転送手段
103
アクセス要求情報設定手段
104
アクセス権情報
200 管理者の端末
201
アクセス要求情報判定手段
202
アクセス要求情報取得依頼手段
203
アクセス要求情報自動判定手段

図１２

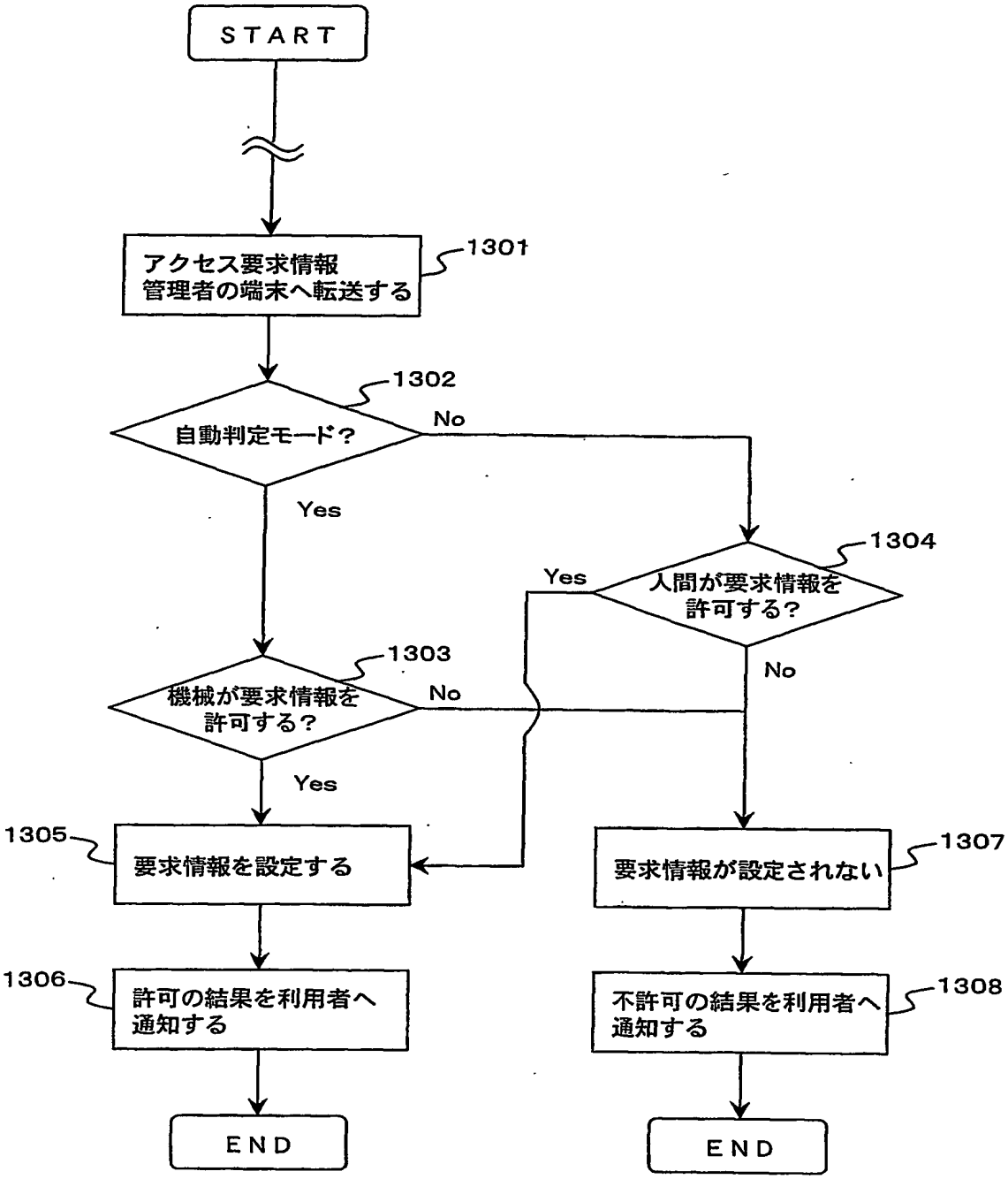

START
アクセス要求情報
管理者の端末へ転送する
1301
1302
自動判定モード？
No
Yes
1304
人間が要求情報を
許可する？
Yes
No
1303
機械が要求情報を
許可する？
No
Yes
1305
要求情報を設定する
1307
要求情報が設定されない
1306
許可の結果を利用者へ
通知する
1308
不許可の結果を利用者へ
通知する
END
END

図１３

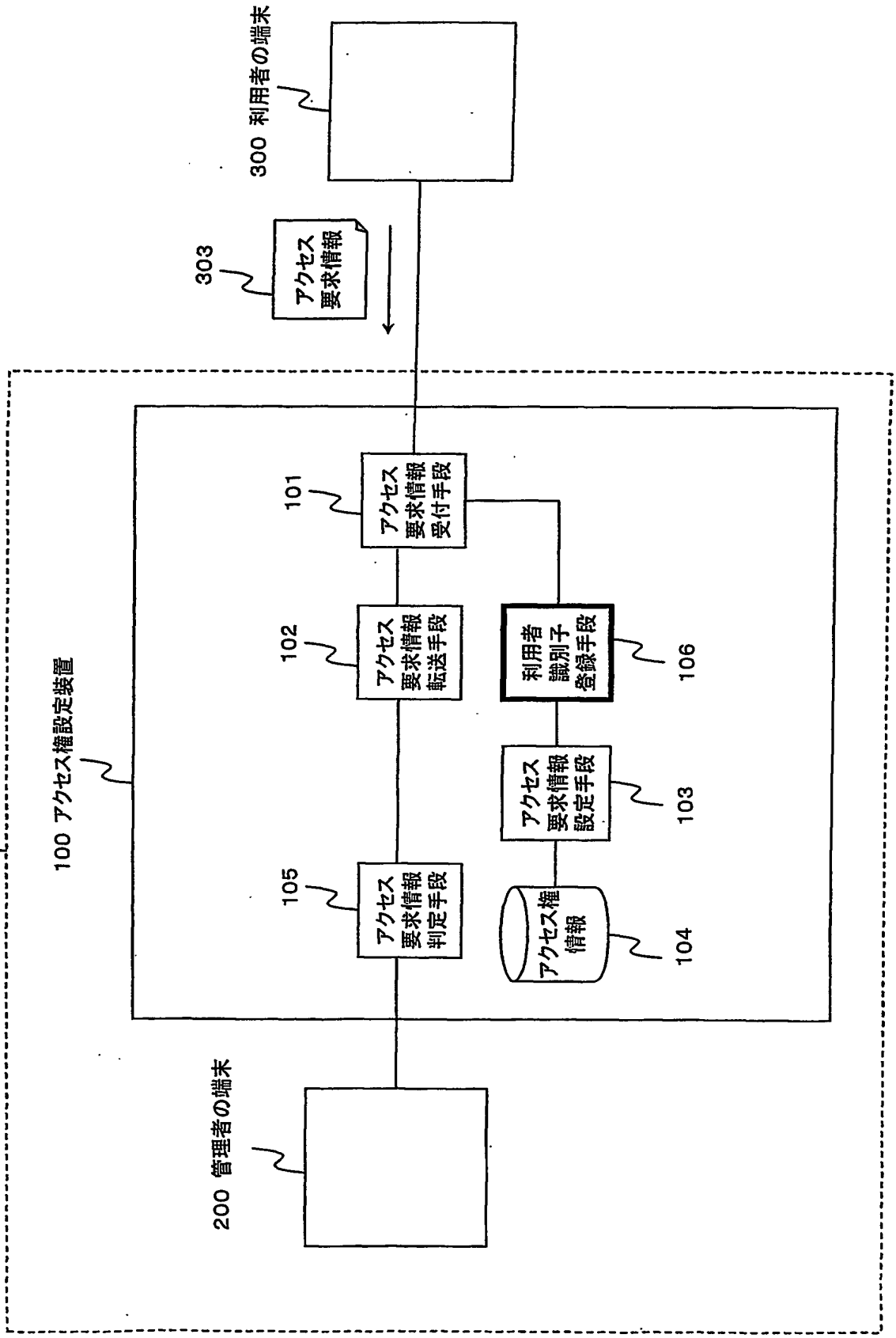

500 ローカルネットワーク
100 アクセス権設定装置
200 管理者の端末
300 利用者の端末
303
アクセス要求情報
101
アクセス要求情報受付手段
102
アクセス要求情報転送手段
105
アクセス要求情報判定手段
103
アクセス要求情報設定手段
106
利用者識別子登録手段
104
アクセス権情報

図１４

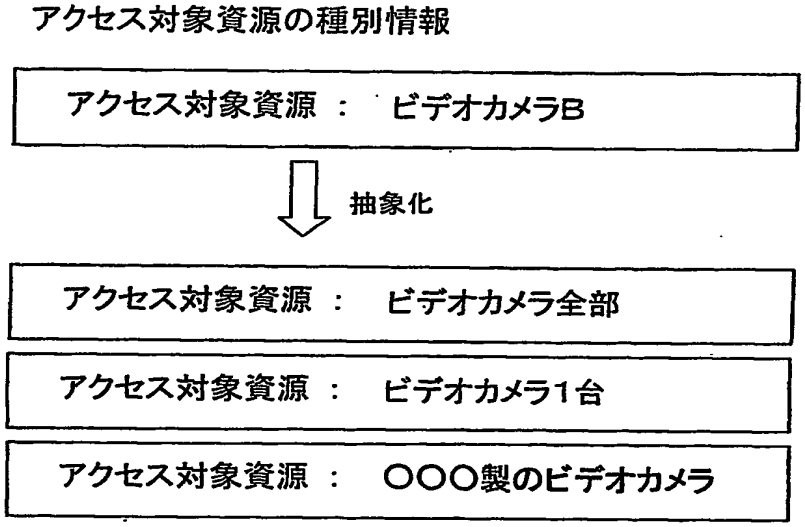
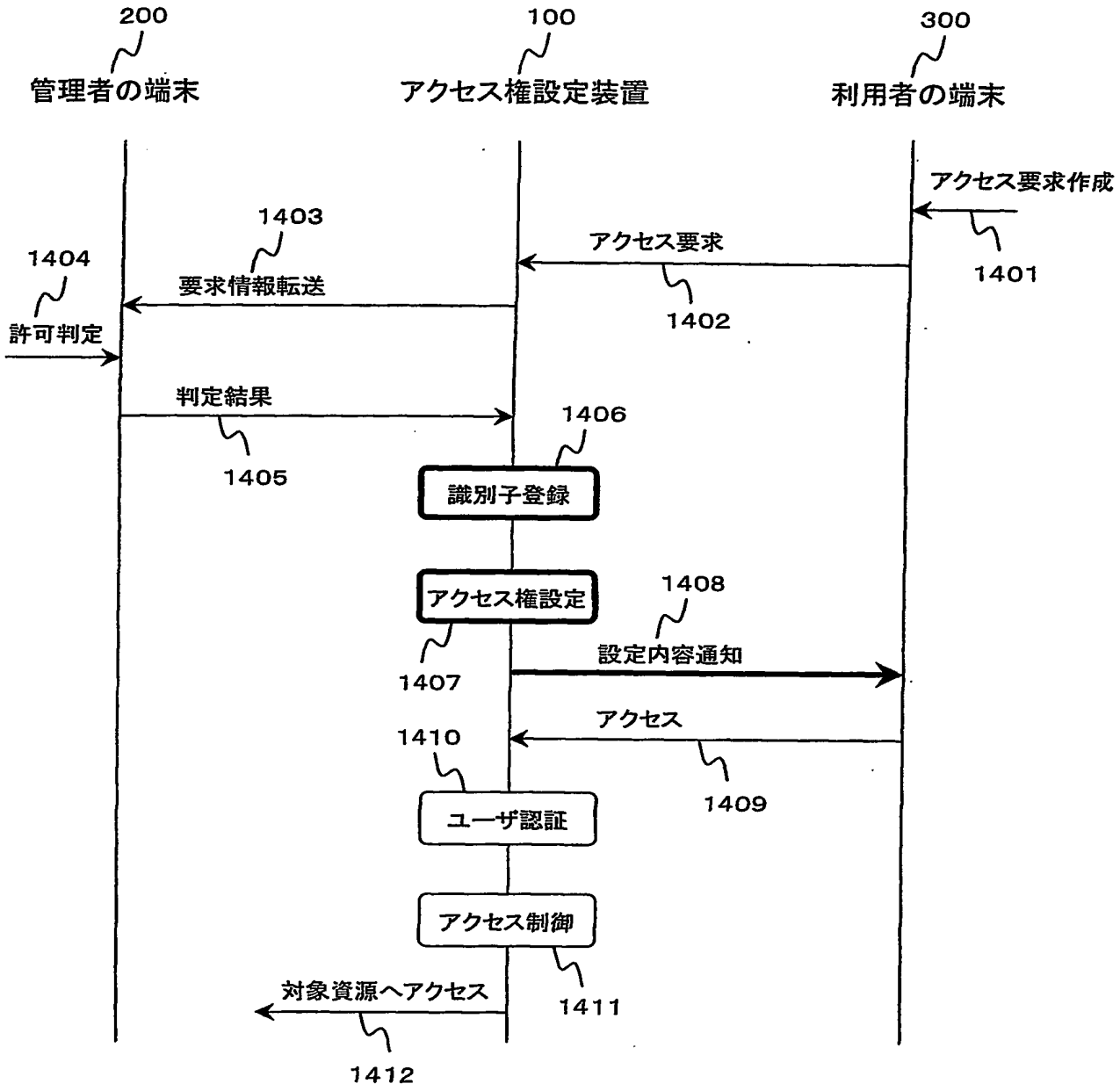

アクセス対象資源の種別情報
アクセス対象資源 ： ビデオカメラB
抽象化
アクセス対象資源 ： ビデオカメラ全部
アクセス対象資源 ： ビデオカメラ1台
アクセス対象資源 ： ○○○製のビデオカメラ

図１５


200
管理者の端末
100
アクセス権設定装置
300
利用者の端末
アクセス要求作成
1401
1403
アクセス要求
1402
1404
要求情報転送
許可判定
判定結果
1405
1406
識別子登録
アクセス権設定
1408
1407
設定内容通知
アクセス
1410
1409
ユーザ認証
アクセス制御
1411
対象資源へアクセス
1412

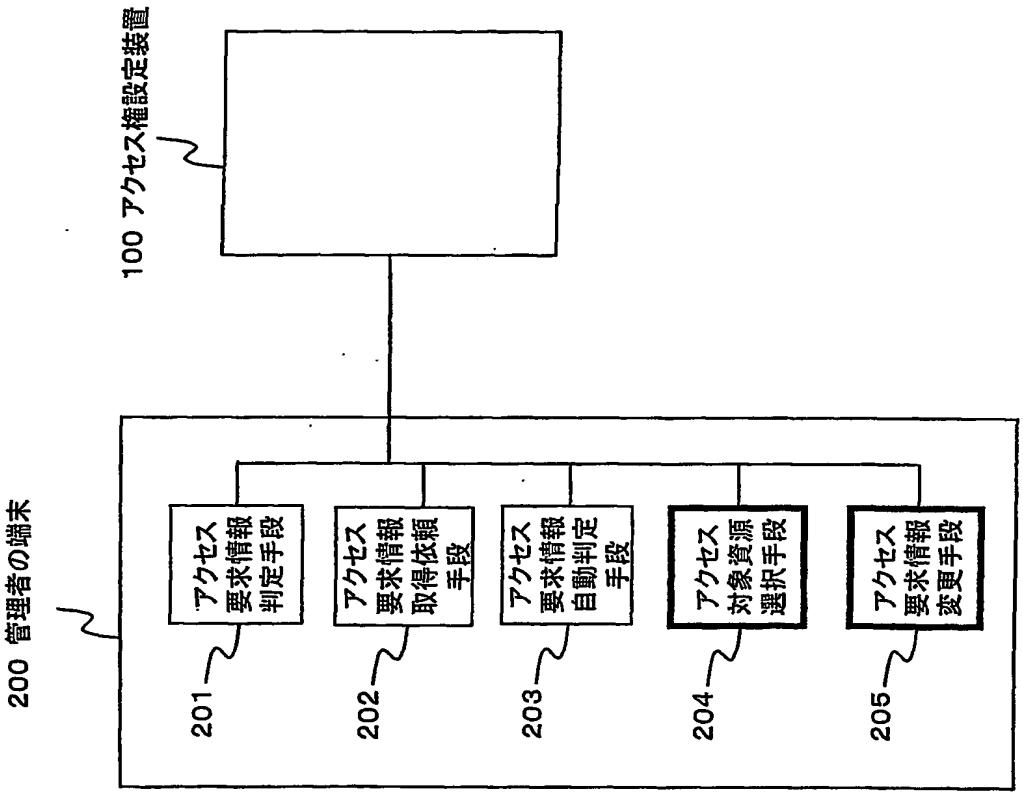

100 アクセス権設定装置
200 管理者の端末
アクセス要求情報判定手段
アクセス要求情報取得依頼手段
アクセス要求情報自動判定手段
アクセス対象資源選択手段
アクセス要求情報変更手段
201
202
203
204
205

図16

図１７

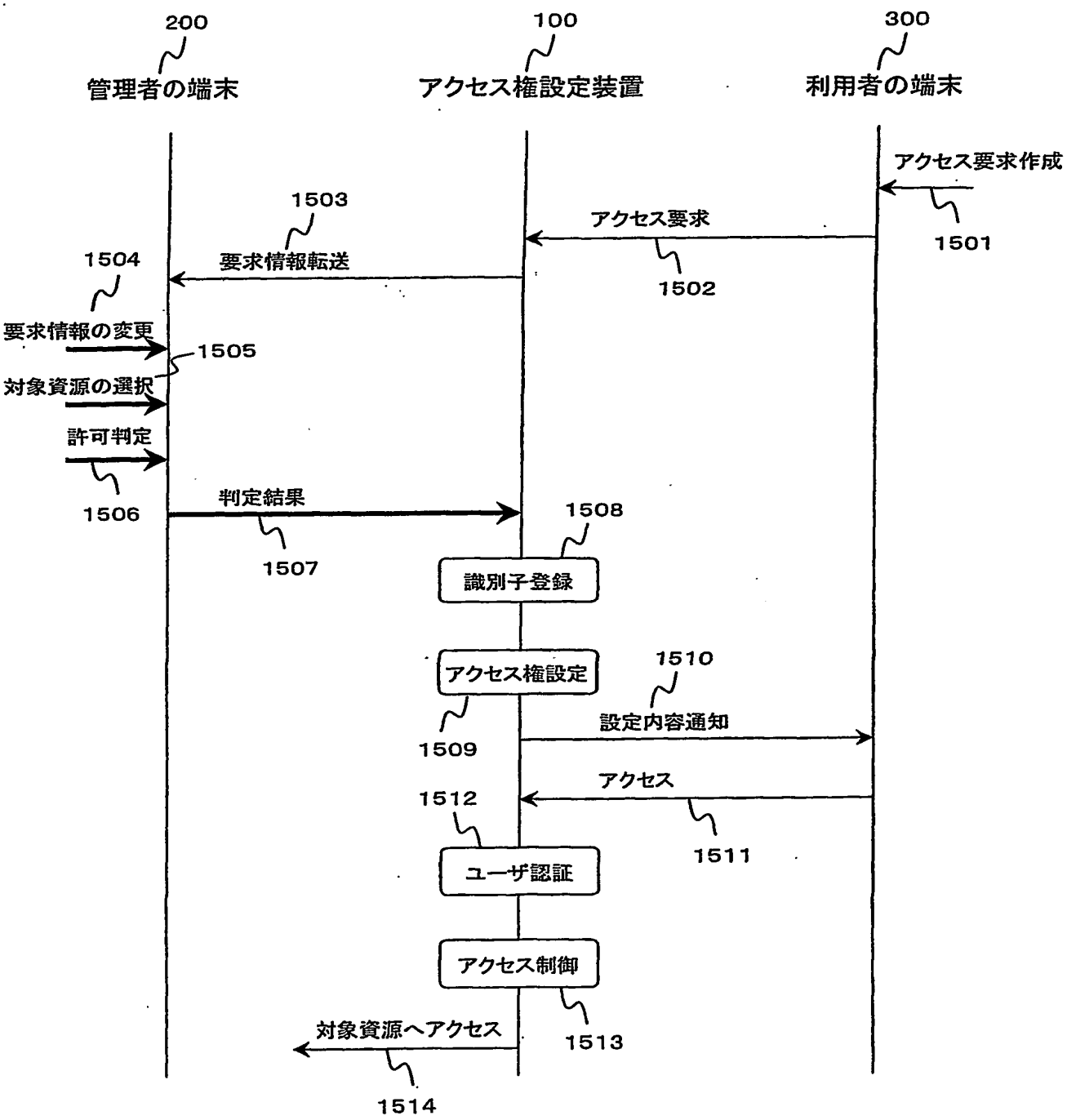

200
管理者の端末
100
アクセス権設定装置
300
利用者の端末
アクセス要求作成
1501
1503
アクセス要求
1502
1504
要求情報転送
要求情報の変更
1505
対象資源の選択
許可判定
1506
判定結果
1507
1508
識別子登録
アクセス権設定
1510
1509
設定内容通知
アクセス
1512
1511
ユーザ認証
アクセス制御
1513
対象資源へアクセス
1514

図１８

内容表示画面の例

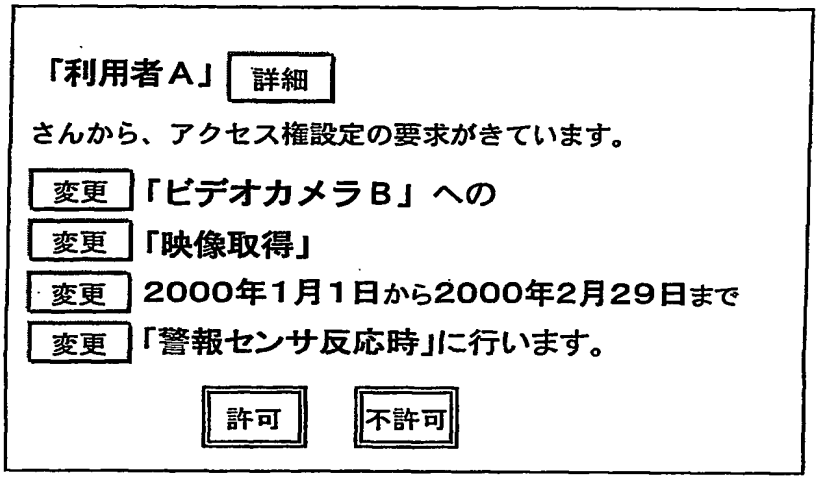


図１９

選択画面の例

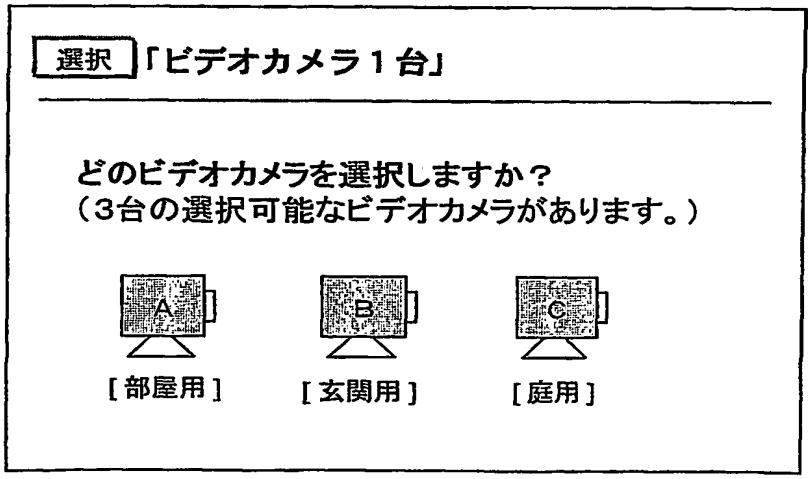


図20

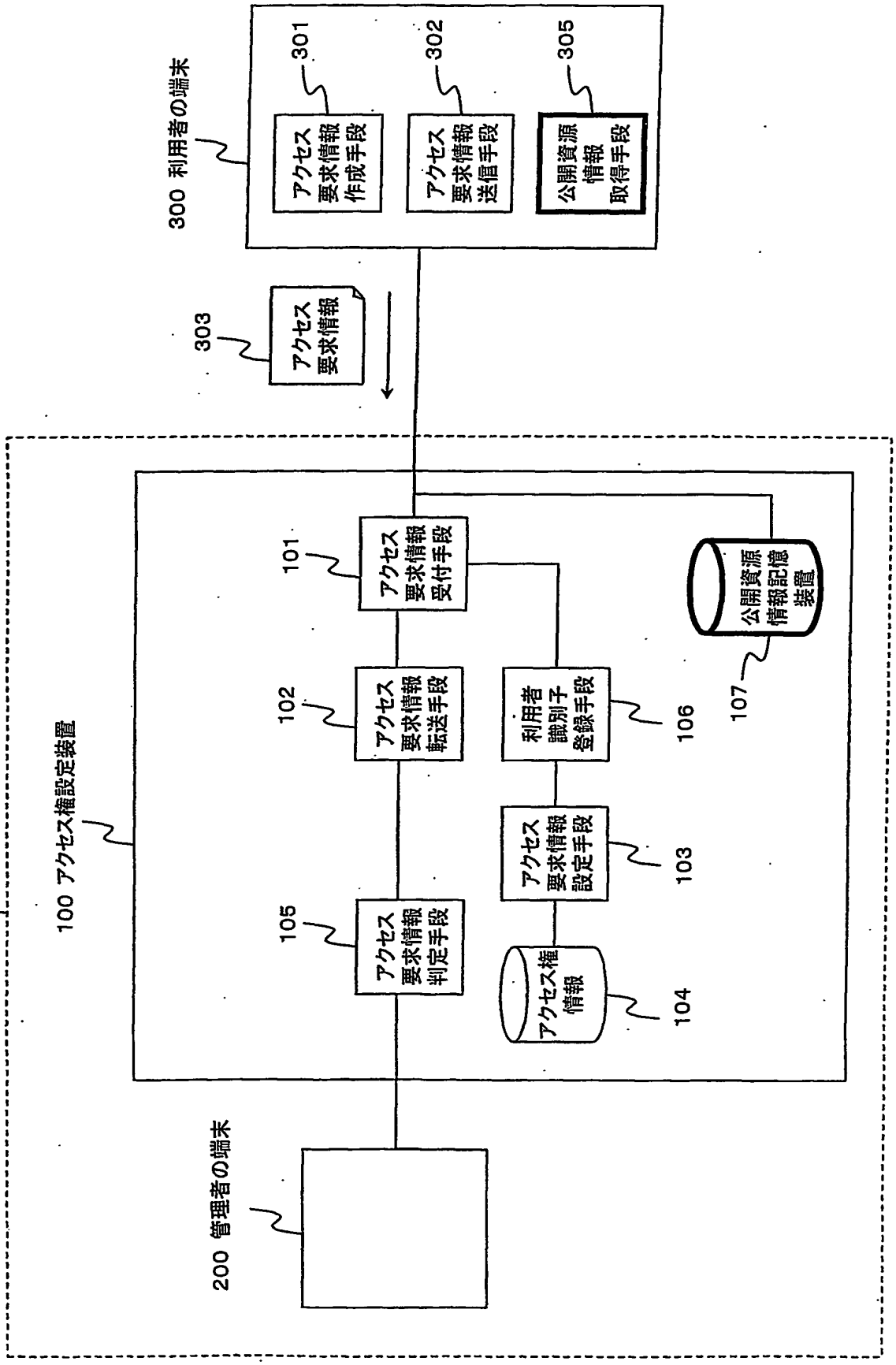

500 ローカルネットワーク
100 アクセス権設定装置
200 管理者の端末
300 利用者の端末
301
302
305
303
アクセス要求情報作成手段
アクセス要求情報送信手段
公開資源情報取得手段
アクセス要求情報
101
102
105
103
104
106
107
アクセス要求情報受付手段
アクセス要求情報転送手段
アクセス要求情報判定手段
アクセス要求情報設定手段
アクセス権情報
利用者識別子登録手段
公開資源情報記憶装置

図２１

公開資源情報の例

[対象資源]	[アクセス内容]
ビデオカメラA	映像取得
ビデオカメラB	ALL
デジタルテレビC	ALL

図２２

公開資源情報の例(種別情報)

[対象資源]
ビデオカメラ
デジタルテレビ

図２３

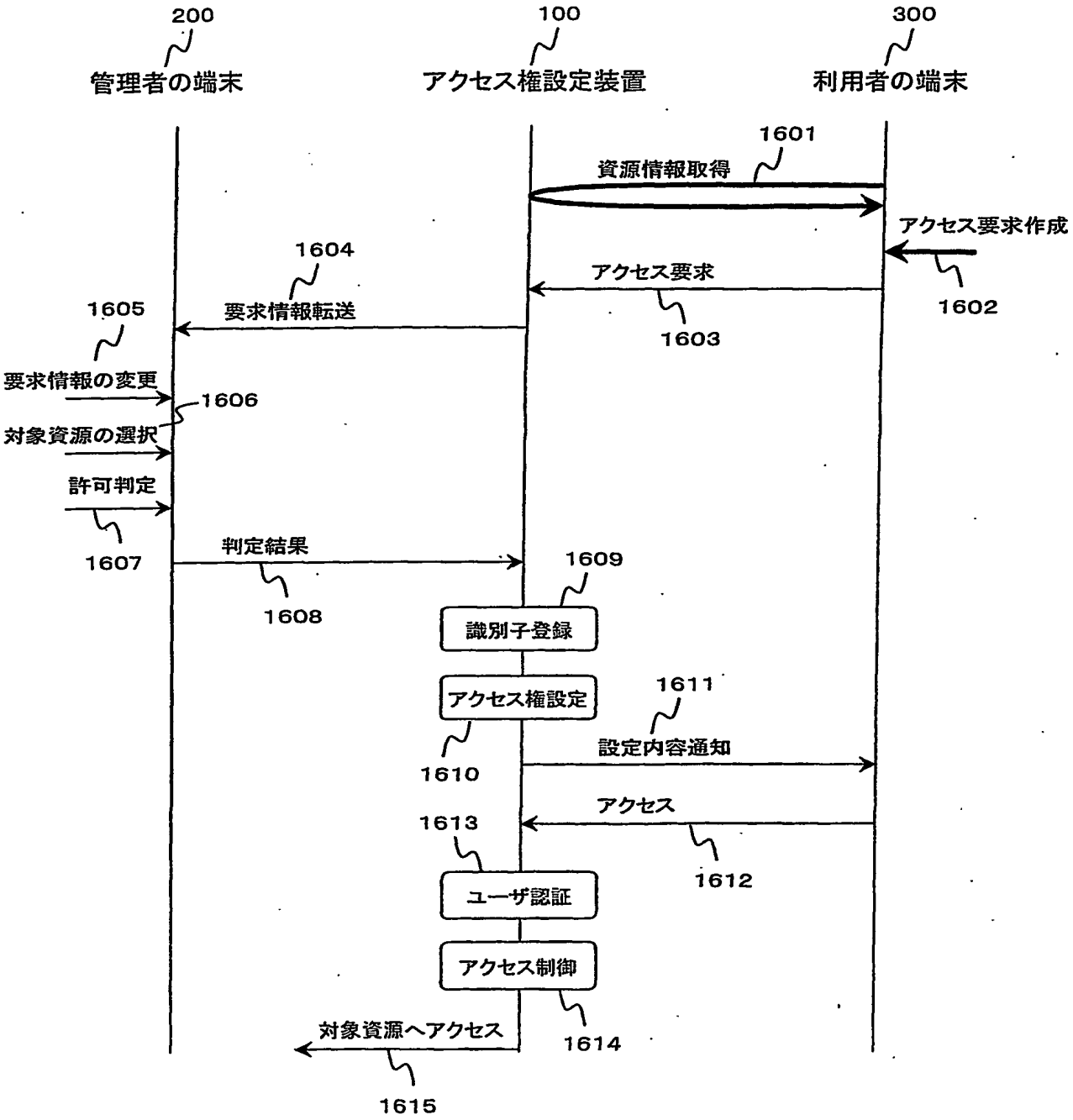

200
管理者の端末
100
アクセス権設定装置
300
利用者の端末
1601
資源情報取得
アクセス要求作成
1604
アクセス要求
1602
1605
要求情報転送
1603
要求情報の変更
1606
対象資源の選択
許可判定
1607
判定結果
1609
1608
識別子登録
アクセス権設定
1611
1610
設定内容通知
アクセス
1613
1612
ユーザ認証
アクセス制御
対象資源へアクセス
1614
1615

図24

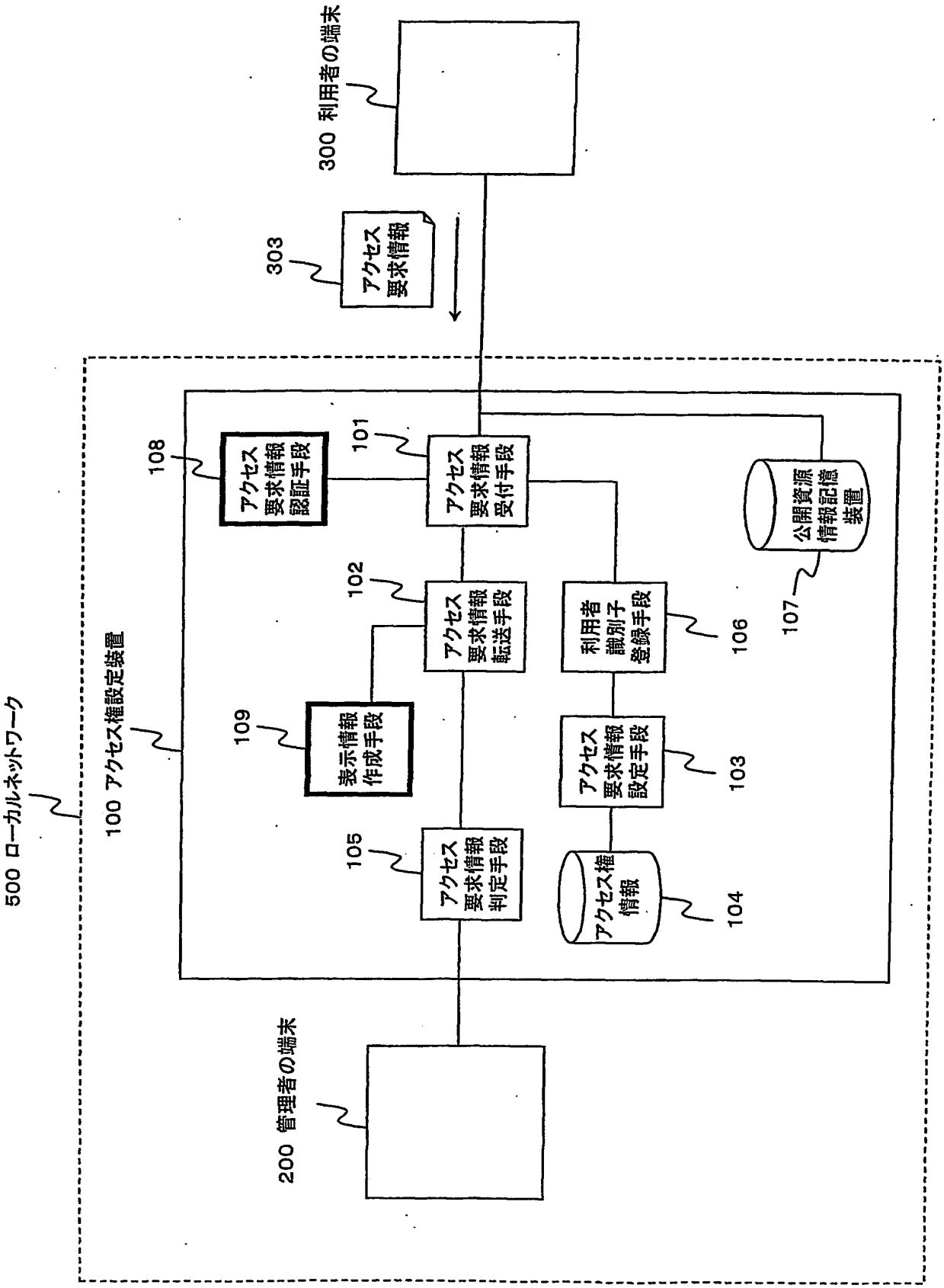

500 ローカルネットワーク
100 アクセス権設定装置
200 管理者の端末
300 利用者の端末
303
アクセス要求情報
101
アクセス要求情報受付手段
102
アクセス要求情報転送手段
103
アクセス要求情報設定手段
104
アクセス権情報
105
アクセス要求情報判定手段
106
利用者識別子登録手段
107
公開資源情報記憶装置
108
アクセス要求情報認証手段
109
表示情報作成手段

図２５

アクセス要求情報（不正情報）の例

［人工言語］

```
<アクセス要求情報>
  <利用者>
    <会社名>警備会社A</会社名>
    <サービス名>遠隔監視サービス</サービス名>
  </利用者>
  <期間>
    <開始>20000101</開始>
    <終了>20000229</終了>
  </期間>
  <アクセス対象資源>0x0004</アクセス対象資源>
  <アクセス内容>0x1020</アクセス内容>
  ・・・・・・
</アクセス要求情報>
```

［自然言語］

警備会社Aの遠隔監視サービスへお申し込み
いただき、誠にありがとうございます。

「1999年12月1日から2000年5月31日まで」の期間、
「ビデオカメラ」の「映像取得」を行いますので、
アクセス権の設定をお願いします。

図２６

変換テーブルの例

[人工言語]	[自然言語]
・対象資源	
0x0004	ビデオカメラ
0x0010	デジタルテレビ
.....	.....
・アクセス内容	
0x1008	映像取得
0x1020	すべての動作
.....	.....

図27

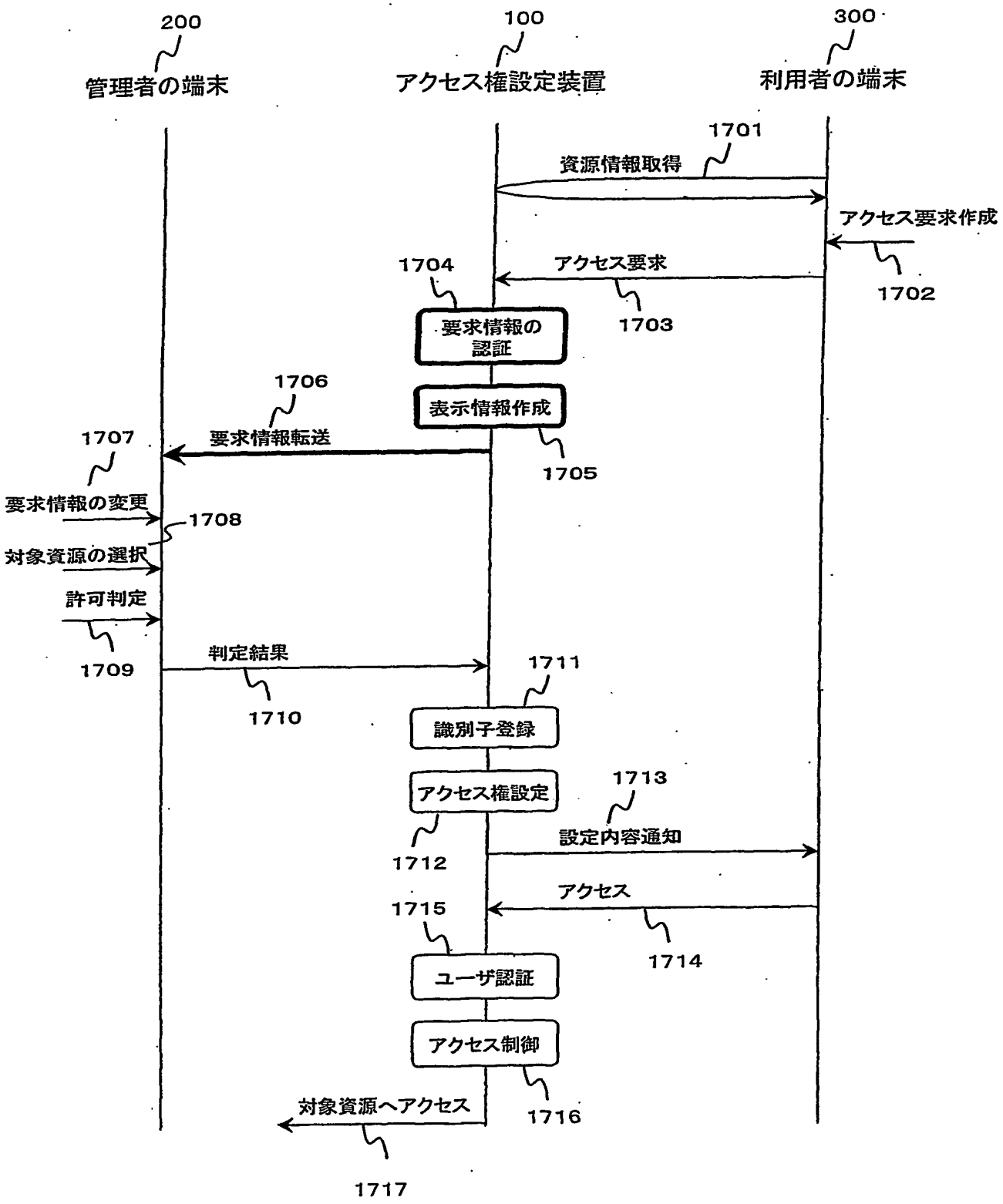

200
管理者の端末
100
アクセス権設定装置
300
利用者の端末
1701
資源情報取得
アクセス要求作成
1702
1704
アクセス要求
1703
要求情報の認証
1706
表示情報作成
1707
要求情報転送
1705
要求情報の変更
1708
対象資源の選択
許可判定
1709
判定結果
1710
1711
識別子登録
アクセス権設定
1713
1712
設定内容通知
アクセス
1715
1714
ユーザ認証
アクセス制御
対象資源へアクセス
1716
1717

図２８

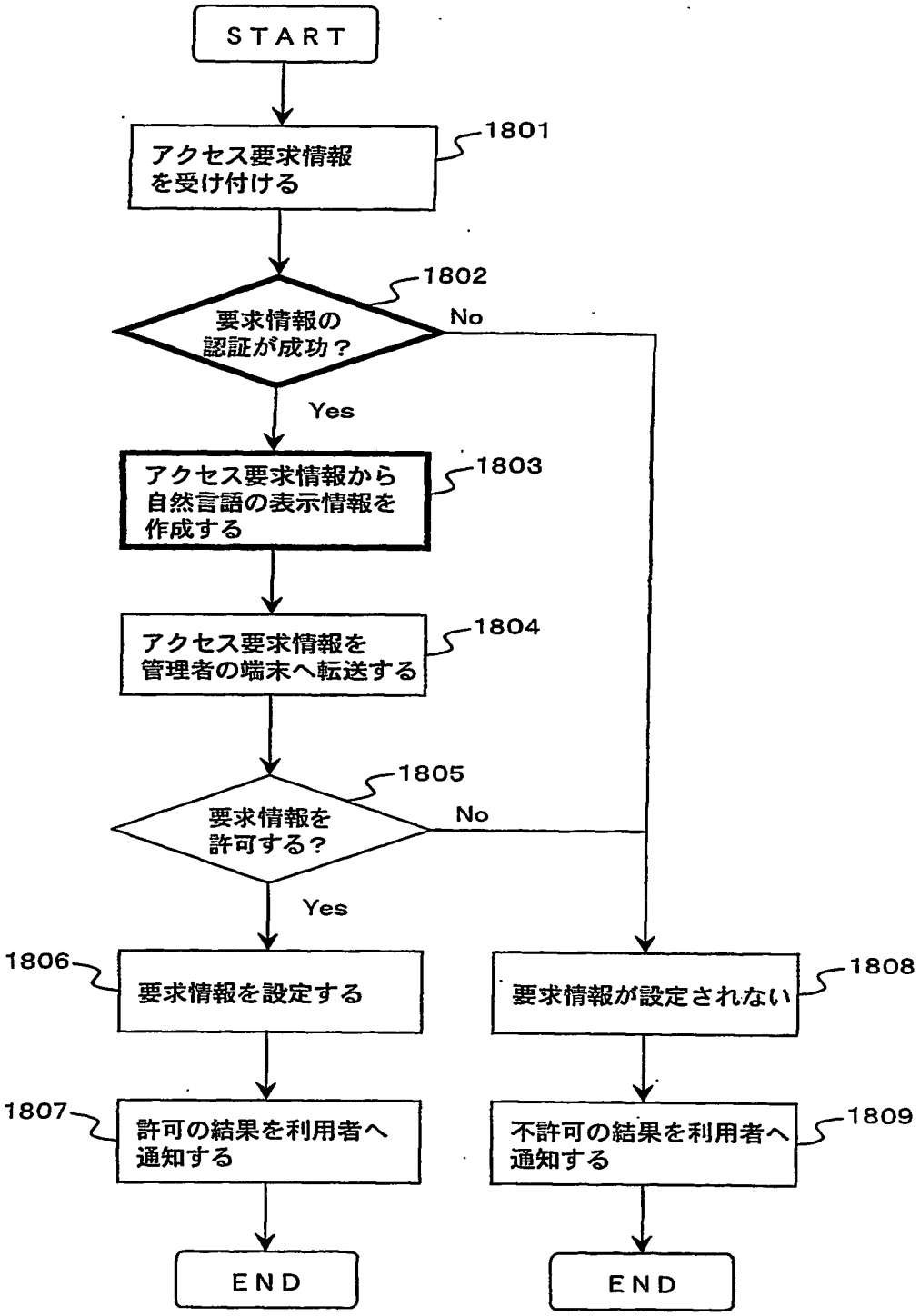

START
アクセス要求情報を受け付ける
1801
要求情報の認証が成功？
1802
No
Yes
アクセス要求情報から自然言語の表示情報を作成する
1803
アクセス要求情報を管理者の端末へ転送する
1804
要求情報を許可する？
1805
No
Yes
1806
要求情報を設定する
1807
許可の結果を利用者へ通知する
END
要求情報が設定されない
1808
不許可の結果を利用者へ通知する
1809
END

図29

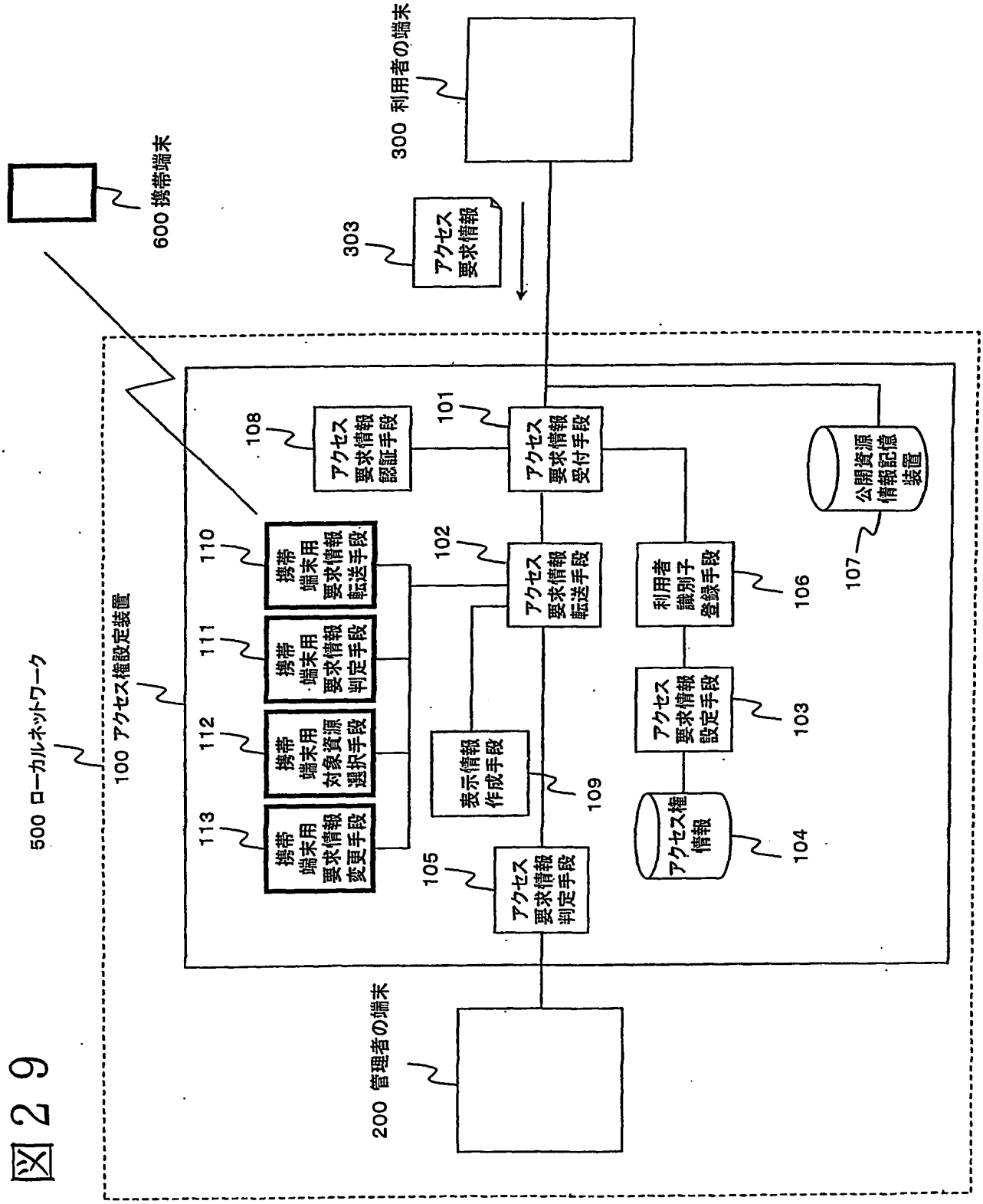
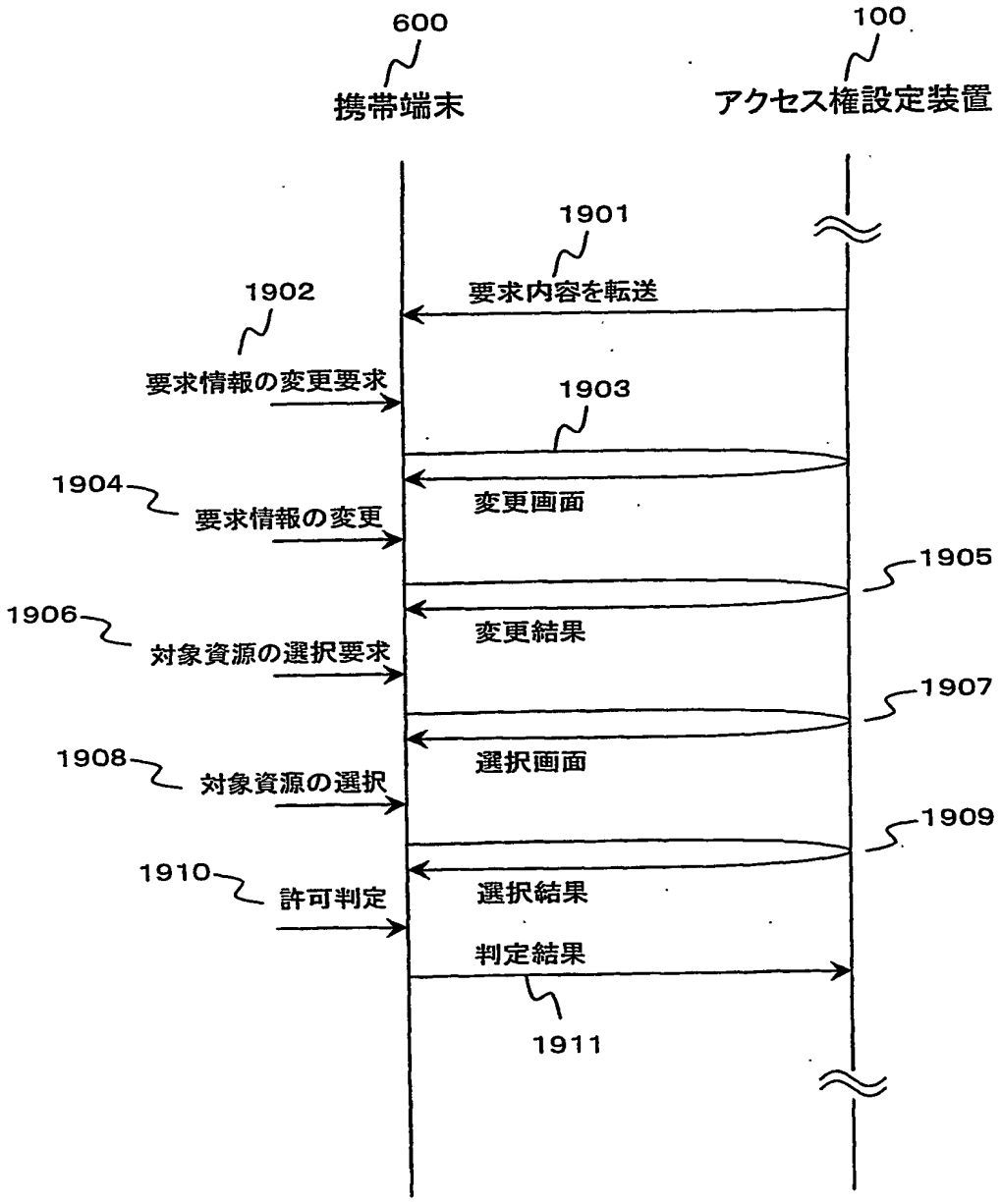

500 ローカルネットワーク
100 アクセス権設定装置
600 携帯端末
300 利用者の端末
303
アクセス要求情報
200 管理者の端末
108
アクセス要求情報認証手段
101
アクセス要求情報受付手段
公開資源情報記憶装置
107
110
携帯端末用要求情報転送手段
102
アクセス要求情報転送手段
利用者識別子登録手段
106
111
携帯端末用要求情報判定手段
112
携帯端末用対象資源選択手段
表示情報作成手段
109
アクセス要求情報設定手段
103
113
携帯端末用要求情報変更手段
105
アクセス要求情報判定手段
アクセス権情報
104

図３０


600
携帯端末
100
アクセス権設定装置
1901
要求内容を転送
1902
要求情報の変更要求
1903
変更画面
1904
要求情報の変更
1905
変更結果
1906
対象資源の選択要求
1907
選択画面
1908
対象資源の選択
1909
選択結果
1910
許可判定
判定結果
1911

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/03515

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/00, G06F13/00, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/00, G06F13/00, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Muryou Build-kei Site de Homepage wo tsukurou", INTERNET magazine, August, 1999, No. 55, pp.294-301	1-14
Y	Oosaka Daigaku Joho Shori Kyouiku Kenkyukai ed. NeXt User Guide Book, 1st printing, Askii Shuppankyoku, 20 June, 1992 (20.06.92), pp. 33-52	1-14
A	Fumi SAKAMOTO, UNIX e no Shoutai, UNIX MAGAZINE, May, 1991, Vol.6, No.5, pp. 151-164	1-14

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 July, 2001 (17.07.01)	21 August, 2001 (21.08.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０１／０３５１５

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl⁷　G06F12/00, G06F13/00, G06F15/00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl⁷　G06F12/00, G06F13/00, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926－1996
日本国公開実用新案公報　1971－2001
日本国登録実用新案公報　1994－2001
日本国実用新案登録公報　1996－2001

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	無料ビルド系サイトでホームページを作ろう, INTERNET magazine, 8月.1999, 第55号, p. 294 - 301	1 - 14
Y	大阪大学情報処理教育研究会 編, NeXT ユーザーガイドブック　第1版, アスキー出版局, 20.6月.1992 (20.06.92), p. 33 - 52	1 - 14
A	坂本　文, UNIXへの招待, UNIX MAGAZINE, 5月.1991, 第6巻, 第5号, p. 151 - 164	1 - 14

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
17.07.01	21.08.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	原　秀人	５Ｎ　９６４４
	電話番号　０３－３５８１－１１０１　内線　３５８５	

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

EP・US

特許協力条約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　P62-0103	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０１／０３５１５	国際出願日（日.月.年）　24.04.01	優先日（日.月.年）　24.04.00
出願人（氏名又は名称）　松下電器産業株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　2　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　1　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報[redacted]　　国際出願番号[redacted]CT／JP01／03515

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷　G06F12/00, G06F13/00, G06F15/00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷　G06F12/00, G06F13/00, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926－1996
日本国公開実用新案公報　1971－2001
日本国登録実用新案公報　1994－2001
日本国実用新案登録公報　1996－2001

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	無料ビルド系サイトでホームページを作ろう, INTERNET magazine, 8月.1999, 第55号, p. 294 - 301	1 - 14
Y	大阪大学情報処理教育研究会 編, NeXT ユーザーガイドブック　第1版, アスキー出版局, 20.6月.1992 (20.06.92), p. 33 - 52	1 - 14
A	坂本　文, UNIXへの招待, UNIX MAGAZINE, 5月.1991, 第6巻, 第5号, p. 151 - 164	1 - 14

☐ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
17.07.01	21.08.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5N	9644
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	原　秀人		
	電話番号　03－3581－1101　内線　3585		

様式PCT／ISA／210（第2ページ）（1998年7月）